

# 試行導入・導入実績公表の手引き

2020年4月

(2021年4月改訂)

独立行政法人 情報処理推進機構

## 目次

1.	はじめに	2
1.1.	背景	2
1.2.	目的	3
1.3.	手引きの対象読者	3
1.4.	手引きの対象製品	3
2.	試行導入の際の注意点	5
2.1.	製品選定におけるポイント	5
2.1.1.	対策すべき課題の決定	5
2.1.2.	導入すべき製品・サービスの決定	5
2.2.	製品試行導入におけるポイント	7
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	10
3.1.	情報公開における注意点	10
3.1.1.	公開可否判断のポイント	10
3.1.2.	試行導入結果の公表内容のポイント	11
3.1.3.	試行導入結果の公表方法・公表対象のポイント	12
4.	試行導入後に実導入する場合のメリット	15
5.	製品ベンダーが準備すべき情報・実施すべき項目	15
5.1.	ユーザー企業による製品選定時	15
5.2.	ユーザー企業による製品導入時	16
5.3.	ユーザー企業による導入実績の公表時	17
6.	用語集・略語集	17

# 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」<sup>1)</sup>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)<sup>2)</sup>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。

### 産業サイバーセキュリティ研究会及びWGの全体構成

- 産業サイバーセキュリティの旗を掲げた研究会及びテーマ毎のWGを設置し、我が国の産業界がサイバーセキュリティに関して直面する課題に対応していく。

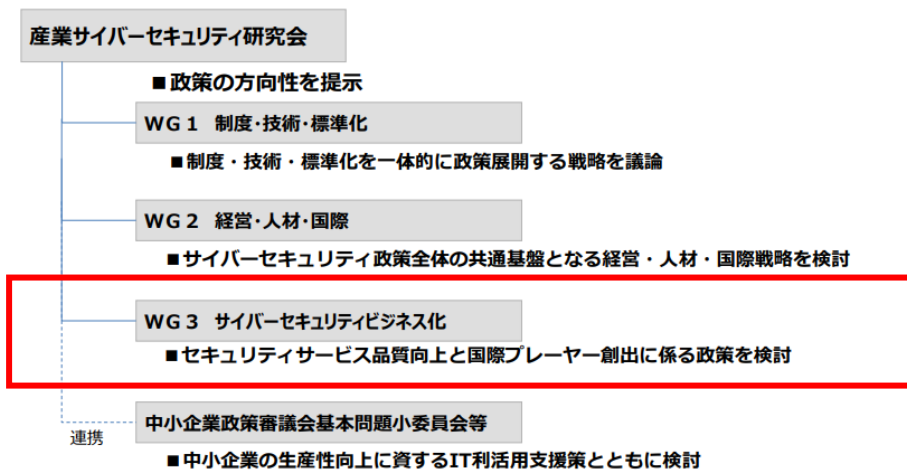


図 1 産業サイバーセキュリティ研究会及びWGの全体構成

(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

<sup>1)</sup> 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](https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/index.html)

<sup>2)</sup> 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](https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/index.html)

品等の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づくり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

上述のような背景を踏まえ、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促すツールという位置づけで、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。また、導入実績の公表結果を受け取った企業が製品を認知し、製品を検討・導入し、導入実績公表といった循環を作り出し、導入実績を増やし、マーケットインを支援することも目的とした。

## 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及び導入実績の公表を検討しているユーザー企業及び製品ベンダーを対象とする。

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」の試行導入及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。加えて、試行導入後に実導入するメリットや、試行導入や導入実績公表時に製品ベンダーで準備すべき事項について解説する。

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事が挙げられる。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事が懸念される。

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 2-1 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	はじ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 2-2 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観点となる。加えて、検知した脅威源の内容や自組織に与える影響を特定できるかどうか観点となる。
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 2-3 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 <sup>3</sup> (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良いかを確認する。
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	既存システムや人材で運用可能か(新しいシステムや人材を確保する必要は無い)、操作方法が既存システムと近しいか等の面から既存環境との親和性を確認する。

<sup>3</sup> 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 <sup>4</sup> /IDS <sup>5</sup> におけるシグネチャ <sup>6</sup> 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 <sup>7</sup> 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	導入及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 2-4 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	導入及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つのフェーズから構成される。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

<sup>4</sup> 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。

<sup>5</sup> 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。

<sup>6</sup> 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。

<sup>7</sup> 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 2-5 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 2-6 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を観点となる。加えて、検知した脅威源の内容や自組織に与える影響を特定できるかどうかを観点となる。
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良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 2-7 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

大前提として、試行導入結果は必ずしも公開する必要があるものではない。導入する製品・サービスによっては、公表することで自組織のセキュリティリスクに繋がる可能性もあり、公表に伴うメリット・デメリットを検討した上で、公表可否を判断することが必要である。公表可否の判断にあたっては、表 3-1 のように導入する製品・サービスの特徴を踏まえて、セキュリティリスクに繋がる可能性があるかを検討する必要がある。また、公表する場合でも、どのような公表方法とするかを検討する必要がある。

表 3-1 製品・サービスの試行導入実績公表により想定されるセキュリティリスク

	製品・サービスの区分	公表により想定されるセキュリティリスク
1	ネットワーク上のセキュリティ脅威の可視化のような間接的な攻撃の防御に寄与する製品	直接的に攻撃に利用されることはないため、公表してもセキュリティリスクに繋がりにくい。
2	アンチウイルスや WAF、IDS/IPS のような攻撃を直接的に防御する製品	公表することでセキュリティリスクに繋がる可能性もある。公表するのであれば、実名ではなく「一部上場企業 A 社」のように抽象度を高めた形での公表が望まれる。
3	システムアーキテクチャに関する製品や SOC の導入実績など、対策の多くが明らかになるような製品・サービス	公表することで対策のレベルが明らかとなり、セキュリティリスクに繋がる可能性があるため、基本的には公表は望まれない。

試行導入結果の公表可否を判断するにあたっては、セキュリティリスクの観点に加えて、公表によるメリット・デメリットを検討する必要がある。試行導入結果の情報公開に伴うメリット・デメリットの例を表 3-2 に示す。メリット・デメリットの検討にあたっては、デメリットを軽減する施策の検討が求められる。その結果を踏まえ、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 3-2 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
<ul style="list-style-type: none"> <li>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</li> <li>セキュリティへの取り組みに積極的なイメージ作り</li> </ul>	<ul style="list-style-type: none"> <li>対策の公表がセキュリティホールになりうるリスク</li> <li>他社からの問い合わせ対応の負荷</li> <li>SNS 等で炎上するリスク</li> </ul>

メリット	デメリット
<ul style="list-style-type: none"> <li>・ 自社の宣伝効果</li> <li>・ セキュリティ攻撃者への牽制(内部不正の防止)</li> <li>・ 製品利用の割引や新しい機能(モジュール)の先行利用等の製品ベンダーからのベネフィット享受</li> </ul>	

### 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<sup>8</sup>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。

公表内容に関する異なる注意点として、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。



**脅威を「遮断」する製品**  
= 脅威は残存しないため  
課題としても解決



**脅威を「検知」する製品**  
= 検知した脅威に対応する  
運用は別途必要

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<sup>9</sup>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期的に行っている場合、組

<sup>8</sup> 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。

<sup>9</sup> 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。

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 3-3 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。

表 3-4 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にあたっては、ユーザー企業があらかじめ公表内容が適切になるように取り決めを求めることが必要である。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 3-5 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 3-6 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

すると不信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 3-7 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. 試行導入後に実導入する場合のメリット

試行導入後に実導入する場合、試行導入時に実施した内容を引継ぎながら実導入することができるため、メリットを享受できる。試行導入の検討においては、試行導入後の実導入も見据えて検討することが望まれる。

表 4-1 試行導入後に実導入する場合のメリット

	項目	内容
1	コストと工数の全体最適化	試行導入をせずに実導入しようとした場合、製品資料から読み取れる情報は限られ、実導入後にモジュールの追加等が発生し、追加コストや手間がかかる可能性がある。そのため、試行導入にて、自社によって適切な導入形態を把握することで結果的に、最適なコストと工数で実導入することができる。
2	製品への納得感	試行導入において、求めている品質や使い勝手等を確認できるため、製品について納得した状態で実導入に移ることができる。
3	実導入の決裁	試行導入時に、製品選定をし、費用対効果も検証済みのため、実導入に向けた社内決裁を進めやすい。
4	安定的な運用	試行導入時と同じサポート体制の場合は、試行導入時の不具合や問題発生時の対応内容を引継ぐことができるため、実導入後は安定的な運用を行うことができる。

## 5. 製品ベンダーが準備すべき情報・実施すべき項目

これまで製品を導入するユーザー企業の視点で整理してきた。本章では製品を開発・販売するベンダーの視点で、準備すべき情報や実施すべき項目を整理する。整理にあたっては、「ユーザー企業による製品選定時」、「ユーザー企業による製品導入時」、「ユーザー企業による導入結果の公表時」の3つのフェーズごとに、準備すべき情報や実施すべき項目を整理する。

### 5.1. ユーザー企業による製品選定時

製品選定時は、自社製品の差別化ポイントをユーザー企業に訴求することが求められる。そのため、製品が解決可能な課題の提示だけでなく、競合製品との比較結果や第三者による評価結果等、客観的に製品の差別化ポイントを判断できる情報を提示することが重要である。

表 5-1 ユーザー企業による製品選定時に準備すべき情報・実施すべき項目

	項目	内容
1	製品が解決可能な	ユーザー企業の抱える課題を解決する製品かどうかを判断



	項目	内容
	課題の提示	できる情報を準備する。
2	製品の導入事例の提示	他のユーザー企業での導入事例があれば、可能な範囲で事例を提示する。
3	競合製品との比較結果の提示	ユーザー企業が製品の判断に使えるよう、競合製品との性能や機能の比較結果を提示する。
4	製品の第三者による評価の提示	製品について第三者機関による評価を受けた結果(受賞歴など)を提示する。
5	製品が導入可能な環境の提示	ユーザー企業の環境で導入可能かどうかを判断できる情報を準備する。システム構成図のようなもので、導入したイメージを提示することが望ましい。
6	導入するために必要な費用・スケジュールの提示	ユーザー企業が想定している予算やスケジュール感と比較できる情報を準備する。導入スケジュールについては、ユーザー企業が何を実施する必要があるかといった導入手順を提示することが望ましい。
7	概算見積もり算出のために必要な情報提示	製品ベンダーが概算見積もりを正確に算出するために、ユーザー企業が提示すべき情報(社員数、使用端末台数等)を提示する。
8	製品導入にあたっての制約条件の提示	ユーザー企業が当該製品を導入するための技術的条件や人員体制等、ユーザー企業が考慮すべき制約条件を準備する。
9	製品ベンダーの将来展望や戦略に関する説明	ユーザー企業が、製品及び製品ベンダーに興味を持つよう促すために、製品開発の背景や市場を踏まえた製品の位置づけ等を提示する。
10	製品に関する問い合わせの対応	ユーザー企業が製品選定する際に、必要な情報等の問い合わせ対応を実施する。

## 5.2. ユーザー企業による製品導入時

製品導入時は、ユーザー企業が製品を利用できるような環境を整えることが必要である。製品の技術情報やマニュアルの提示や導入に必要な環境の構築だけでなく、製品に対する問い合わせの対応を実施することが求められる。

表 5-2 ユーザー企業による製品導入時に準備すべき情報・実施すべき項目

	項目	内容
1	製品の技術情報・マニュアルの提示	製品に関する技術情報や製品利用時に必要なマニュアルを提示する。

	項目	内容
2	導入のための体制の構築、スケジュールの策定	導入までの体制やスケジュールをユーザー企業へ提示する。
3	導入に必要な環境構築	導入のための環境構築が必要であれば、環境構築を実施する。
4	製品に関する問い合わせの対応	ユーザー企業が製品導入する際に、必要な情報等の問い合わせ対応を実施する。

### 5.3. ユーザー企業による導入実績の公表時

ユーザー企業が導入実績を公表するとなった場合、公表内容の意識合わせを実施する必要がある。この実施にあたっては、「3.1.1. 公開可否判断のポイント」で示したとおり、公表によるユーザー企業へのセキュリティリスクの可能性を踏まえる必要がある。

表 5-3 ユーザー企業による導入実績の公表時に準備すべき情報・実施すべき項目

	項目	内容
1	公表内容の確認	公表前に公表内容が適切かを確認する。
2	製品に関する問い合わせ対応	公表結果を閲覧した他のユーザー企業が直接製品提供企業へ問い合わせることが想定されるため、問い合わせ対応を実施する。

## 6. 用語集・略語集

IPS/IDS:

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

SOC:

Security Operation Center、ネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスをを行う組織を指す。

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

以上