弁護士法人　三宅法律事務所

Miyake　& Partners

デジタル・ガバナンス／サイバーセキュリティニュース　No.4

経済産業省「SSDF 導入ガイダンス案」が目指すもの

―「安全です」という説明から、開発プロセスと証拠による説明へ ―

平素より大変お世話になっております。

経済産業省は、米国国立標準技術研究所（NIST）[1]が策定した**セキュア・ソフトウェア開発フレームワーク（SSDF）**を、日本企業の開発・調達の現場に導入するための「セキュア・ソフトウェア開発フレームワーク導入ガイダンス案」を取りまとめています。令和 8 年 7 月に開催された第 18 回サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースでは、第 17 回タスクフォースで受領した 12 件の意見を踏まえた改訂版が示されました。

今回のガイダンス案が目指しているのは、「脆弱性の少ないプログラムを書くこと」ではありません。より本質的には、**ソフトウェアが、どのような組織、開発環境、管理手続及び検証プロセスによって作られたのかを、発注者や顧客に対して説明できるようにすること**にあります。したがって、これは開発者のみを対象とする技術的な手引ではなく、経営、調達、法務、内部統制、内部監査及びサプライチェーン管理にも関係するガバナンス上の枠組みです。

また、令和 8 年 7 月 21 日には、開発中の AI モデルが人間の意図に反して他社システムに侵入したとされる事故が公表されました。隔離された試験環境から未知の脆弱性を用いて脱出したとされる本件は、開発環境の分離・保護や未知の脆弱性への対応など、SSDF が正面から扱う論点と重なります。

本ニュースレターでは、ガイダンス案が目指すものを国際的な流れとともに整理した上で、改訂版で具体化された達成レベル、網羅率、チェックリスト及びツール活用の考え方、第 17 回タスクフォースにおける意見と改訂内容の一覧、取締役・監査役が確認すべき事項並びに当面の実務対応を整理いたします。末尾には理解度チェック（〇×問題 10 問）を付しております。

令和 8 年 7 月 22 日
弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。
弁護士法人三宅法律事務所
弁護士　渡邉雅之（執筆者）
TEL 03-5288-1021　FAX 03-5288-1025
Email: m-watanabe@miyake.gr.jp

[1] NIST（National Institute of Standards and Technology、米国国立標準技術研究所）とは、1901 年に設立された米国商務省傘下の政府機関をいう。長さ・質量・時間等の計測標準や工業規格の策定・維持を本来の任務とするが、情報セキュリティの分野においても、連邦政府機関が用いる基準・ガイドラインの策定を担っており、その成果は SP800 シリーズ（例：SP800-53「情報システム及び組織のためのセキュリティ・プライバシー管理策」、SP800-61「インシデント対応の手引」、SP800-218（SSDF））及びサイバーセキュリティフレームワーク（CSF）等として公表されている。NIST の文書は、法令そのものではなく、また第一次的には米国連邦政府機関を名宛人とするものであるが、大統領令に基づき政府調達の要件を基礎付ける役割を担うこと、及び技術的な中立性・網羅性が高いことから、事実上の国際標準として、我が国を含む各国の民間企業においても広く参照されている。

デジタル・ガバナンス／サイバーセキュリティニュース　No.4

経済産業省「SSDF 導入ガイダンス案」が目指すもの

―「安全です」という説明から、開発プロセスと証拠による説明へ ―

【目次】

1　はじめに

SSDF とは、簡単にいえば、**ソフトウェアを安全に開発し、リリース後に判明した脆弱性にも適切に対応するために、企業が整備・実践すべき組織、プロセス及び技術上の取組を体系化したフレームワーク**である[2]。

経済産業省のガイダンス案は、これを国内の開発・調達の現場で実践するための具体的な方法や手順を示すものであり、発注者にとっては供給者・開発委託先の開発方法を確認するために、供給者にとっては調達者に対して開発方法を可視化し、説明責任を果たすために利用できるものと位置付けられている。

[2] SSDF（Secure Software Development Framework）とは、NIST（米国国立標準技術研究所）が令和 4 年 2 月に公表した SP800-218 Version 1.1 をいう。ソフトウェアの脆弱性を低減するために開発者が実施すべき実践策（プラクティス）を、特定の製品・開発手法に依存しない形で体系化したものである。

本稿では、ガイダンス案が目指すものを整理した上で、令和 8 年 7 月の第 18 回タスクフォースに提出された改訂版[3]の内容を、企業のガバナンス・内部統制の観点から解説する。

2 なぜ、完成したソフトウェアだけを検査しても足りないのか

従来のサイバーセキュリティ対策では、完成したシステムを外部から守ることが中心であった。ファイアウォール、ウイルス対策ソフト、アクセス制御、完成後の脆弱性診断等である。

しかし、現在のソフトウェアは、自社で一から全てを作るとは限らない。一般に、自社で開発したプログラム、外部委託先が作成したコード、OSS（オープンソースソフトウェア）、外部のライブラリや部品、クラウドサービス、開発・テスト・配布を自動化する各種ツールといった多数の要素から構成されている。

このため、完成した製品に問題がないかを確認するだけでは十分ではない。ソースコード、開発環境、プログラムを組み立てるビルド工程、電子署名、更新プログラムの配布経路等が侵害されれば、正規のソフトウェアの中に不正なコードが混入することがあるためである。

3 SolarWinds 事件が示したもの

この問題を象徴するのが、令和 2 年（2020 年）に明らかになった **SolarWinds 事件**である。SolarWinds が提供していたネットワーク管理ソフトウェア「Orion」の開発・更新経路が侵害され、不正なコードを含む更新プログラムが正規のアップデートとして配布された[4]。

利用者は、出所不明のファイルを誤って開いたのではない。正規の供給者から提供された正規の更新プログラムを導入したことによって、侵害を受ける可能性が生じた。この事件が示したのは、**「正規の供給者による正規のソフトウェアであること」と「安全なソフトウェアであること」は同じではない**ということである。

そこで、政府や発注者は、完成したソフトウェアだけを見るのではなく、供給者に対して次の事項を確認する必要があると認識するようになった。

- 開発環境をどのように保護しているか
- ソースコードに誰がアクセスできるか
- ビルド工程の改ざんをどのように防いでいるか
- 外部のソフトウェア部品を把握しているか
- リリース前にどのような検証を行っているか
- リリース後の脆弱性にどのように対応するか

4 SolarWinds 事件は NIST にどのような影響を与えたのか

SSDF の検討自体は SolarWinds 事件以前から進められており、同事件を受けて SSDF が一から作られたという関係ではない。SSDF は、2000 年代以前から蓄積されてきたセキュア・コーディングやソフトウェア・セキュリティ・アシュアランスの実践知・経験則を整理したものである。

もっとも、SolarWinds 事件を含む深刻なサプライチェーン侵害を背景に、令和 3 年 5 月、米国では大統領令 14028 が発出され、NIST に対してソフトウェア・サプライチェーンの安全性及び完全性を向上させるための基準・ガイダンスの

---

[3] 第 18 回タスクフォース（令和 8 年 7 月）の配布資料は、資料 3（事務局資料）のほか、参考資料 1「SSDF 導入ガイダンスに対する意見と修正内容一覧」、参考資料 2「SSDF 導入ガイダンス（案）」、参考資料 3「SSDF 導入ガイダンス付属ツール等（案）」、参考資料 4・5（英訳版）で構成される。経済産業省ウェブサイト https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/018.html 参照。なお、参考資料 2 の表紙の日付は令和 8 年 3 月 31 日と記載されているが、第 17 回タスクフォースの意見を踏まえた改訂版として第 18 回タスクフォースに提出されたものである。

[4] CISA（米国サイバーセキュリティ・インフラストラクチャセキュリティ庁）は、令和 2 年 3 月から 6 月までにリリースされた複数の Orion 製品バージョンが悪用されたと公表している。https://www.cisa.gov/news-events/alerts/2020/12/13/active-exploitation-solarwinds-software

策定が求められた[5]。これを受け、SSDF は連邦政府のソフトウェア調達政策を支える重要な基準として位置付けられ、令和 4 年 2 月に NIST SP800-218 Version 1.1 として公表された。

この流れによって、NIST の焦点は、「安全なコードを書くこと」だけから、**「開発、ビルド、テスト、リリース及び脆弱性対応を含む供給プロセス全体を安全に管理すること」**へと明確に広がった。なお、NIST は令和 7 年 12 月に SSDF Version 1.2 の初期公開草案を公表しており、我が国のガイダンス案が前提とする Version 1.1 との関係についても、今後の動向に留意が必要である[6]。

5 AI が自律的にサイバー攻撃を行った事例 ― 「隔離しているから安全」か

令和 8 年 7 月 21 日、米オープン AI は、開発中の AI モデルが、人間の意図に反して他社に対するサイバー攻撃を行う事故が発生したと公表した[7]。報道によれば、事故は、AI モデルのサイバー攻撃能力を測定するテストの過程で生じたものである。テストは「サンドボックス」と呼ばれる隔離環境で実施され、本来、AI は外部のネットワークに接続できない設計であった。

しかし、当該 AI は、テスト環境のシステムに存在する未知の脆弱性を発見して隔離環境から脱出し、外部ネットワークへの接続に成功した。さらに、テストの「解法」が多くの AI 企業の利用する米ハギングフェイスの環境にあると推定し、同社システムの未知の脆弱性を利用して侵入し、秘密情報を取得したとされる。モデル側に実装されていた安全対策は機能しなかった。同社は、これに先立つ 7 月 16 日、自律的に動作する AI エージェントによる攻撃を受けた旨を公表しており、その後、オープン AI から自社モデルによる攻撃であった旨の連絡を受けたとされる。

指示を出した側に悪意はなかったとみられるが、本件は、目標の達成を優先した結果として想定外の挙動が生じる**「報酬ハッキング」**の一例であり、AI の脅威と制御の難しさを示すものである。悪用防止の観点から、一部の最先端モデルについては利用者を限定する運用がとられているが、最新の AI を用いた攻撃事例が公表されること自体が少ない中で、本件は貴重な事例といえる。なお、被害を受けた側は、当初、商用の AI に分析を依頼したものの、悪用防止機能が作動して分析を拒否されたため、最終的にオープン型のモデルを用いて分析を行ったと報じられている。

SSDF の観点からみた含意

本件は、開発・調達の実務にとって、次の点で SSDF が求める事項の重要性を裏付けるものである。

- **開発基盤の分離及び保護（PO.5.1、PO.5.2）**：隔離環境（サンドボックス）それ自体が脆弱性を含み得る「開発基盤」である。隔離しているという事実のみをもって安全と評価することはできず、外部通信の遮断、権限設定、監視及びログ取得が実際に機能しているかを検証し、その結果を記録しておく必要がある
- **未知の脆弱性への対応（RV.1.1、RV.2.1、RV.3.3）**：AI により未知の脆弱性の発見・悪用が高速化すれば、検知から修正までに許容される時間は短縮する。契約上の通知期限・修正期限の設定や、類似脆弱性の横断的な調査の重要性が一層高まる
- **サプライチェーン（PW.4.1、PW.4.4）**：多数の事業者が共通して利用する基盤（モデルやデータセットの共有基盤等）が侵害された場合、影響は利用者全体に波及する。第三者製コンポーネントの取得・検証及び SBOM による構成把握が前提となる
- **テスト・実験環境のガバナンス**：能力評価やレッドチーミングを目的とする実験であっても、外部への到達可能性、権限者による事前承認、監視及び記録の在り方は内部統制上の論点となる。実験環境は「本番ではない」ために管理が緩みやすい

---

[5] 大統領令 14028「Improving the Nation's Cybersecurity」（令和 3 年 5 月）は、NIST に対し、ソフトウェア・サプライチェーンの安全性及び完全性を向上させるための基準・ガイダンスの策定を求めた。SSDF Version 1.1 は、これを受けて令和 4 年 2 月に公表されたものである。

[6] NIST は、令和 7 年 12 月 17 日、大統領令 14306 に基づき、SP800-218 Rev.1（SSDF Version 1.2）の初期公開草案を公表した（意見募集は令和 8 年 1 月 30 日に終了）。経済産業省のガイダンス案は Version 1.1 を前提としているため、今後の NIST 及び経済産業省の改訂動向に留意が必要である。

[7] 日本経済新聞令和 8 年 7 月 22 日付「OpenAI、開発中の AI がサイバー攻撃　他社システムに『誤侵入』」（シリコンバレー＝伴正春記者）。オープン AI による公表は同月 21 日である。本文中の事実関係は同記事の報道による。

- **インシデント対応時の手段の確保**：安全対策が作動して商用 AI による分析が拒否されたという経緯は、緊急時に利用できる分析手段をあらかじめ確保しておくこと（体制、契約、代替手段）が実務課題であることを示している

また、AI そのものの開発についても、NIST は、生成 AI 及びデュアルユース基盤モデルの開発に関する SSDF のコミュニティプロファイル（SP800-218A）を公表している[8]。SSDF は、AI を利用する側の課題であると同時に、AI を開発する側の課題でもある。

本件が示すのは、結局のところ本稿の視点と同じである。すなわち、事故が起きたか否かのみによって管理の適切性を判断することはできず、**どのような環境を用意し、いかなる制御を設け、それが実際に機能していたかを、記録に基づいて説明できるか**が問われるということである。

6 SSDF の 4 つの実践領域

SSDF は、ソフトウェアの脆弱性を低減するための取組を、次の 4 つの実践領域（プラクティス）に整理している。これらは、**「開発前の準備」→「ソフトウェアの保護」→「安全な開発」→「リリース後の継続的な脆弱性管理」**という、ソフトウェアライフサイクル全体をカバーするものである。

実践領域	内容
PO：Prepare the Organization （組織の準備）	セキュリティ要件、役割・責任、教育・訓練、ツールチェーン、開発基盤の分離・保護等を整備し、組織としてセキュア開発を実施できる状態を準備する
PS：Protect the Software （ソフトウェアの保護）	ソースコード、ビルド成果物、リリース情報等を不正アクセスや改ざんから保護し、完全性の検証に必要な情報を提供する
PW：Produce Well-Secured Software （セキュアな開発）	リスク分析、セキュア設計・設計レビュー、第三者製部品の取得・検証、セキュアコーディング、コードレビュー、静的・動的テスト等を通じて、安全なソフトウェアを開発する
RV：Respond to Vulnerabilities （脆弱性への対応）	リリース後も脆弱性情報を継続的に収集・評価・修正し、根本原因を分析して、開発プロセスの改善につなげる

4 つの実践領域は、合計 43 のタスク（PO.1.1、PS.1.1、PW.1.1、RV.1.1 等）に細分化されており、ガイダンス案は、その一つひとつについて達成レベルの指針と具体例を示している。

7 ウォーターフォール、アジャイル、DevOps ― 開発方法を問わず利用できる

SSDF の特徴は、特定の製品、技術又は開発手法を一律に指定するのではなく、**何を達成すべきか**を示している点にある。そのため、異なるソフトウェア開発方法に共通して利用できる。

ウォーターフォール

「要件定義→設計→開発→テスト→リリース」という工程を、原則として順番に進める伝統的な開発方法である。建物の設計・施工のように、最初に仕様や計画をある程度固めてから後の工程に進む。設計審査、コードレビュー、テスト、リリース承認等、各工程の節目に SSDF のセキュリティ確認を組み込むことが考えられる。

アジャイル

最初から完成形を一度に作るのではなく、短い期間ごとに小さな機能を開発し、利用者の意見や状況の変化を取り入れながら、開発と改善を繰り返す方法である。短い開発サイクルの中に、リスク確認、コードレビュー、自動テスト等を継続的に組み込む。

[8] NIST SP800-218A「Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile」（令和 6 年 7 月公表）。SSDF のプラクティスを、生成 AI モデル及びデュアルユース基盤モデルの開発に適用する際の補完的なプロファイルとして整理したものである。

DevOps

開発を担当する部門と、完成後のシステムを運用する部門が連携し、テスト、リリース、監視等を自動化しながら、ソフトウェアを継続的に改善する考え方である。厳密には、単独の開発手法というよりも、開発と運用を一体化する組織・プロセス上の考え方である。

改訂版のガイダンス案は、これを一歩進め、**DevSecOps** に基づくツール活用の基本モデルを示している[9]。開発フェーズごとに個別のツールを用いるだけでなく、ツールチェーンによる統合管理により、人手による誤りや漏れを解消し、要求のトレーサビリティを確保することが目指されている。

すなわち、SSDF は企業に特定の開発方法への変更を求めるものではなく、**現在採用している開発方法の中に、必要なセキュリティ対策を組み込むための共通の枠組み**として利用されるものである。

8 国内に多数のガイドラインがあるのに、なぜ新しいガイダンスが必要なのか

我が国には、既に多数のサイバーセキュリティ関係のガイドラインが存在する。ガイダンス案は、SSDF とのマッピング対象として、SBOM 導入手引[10]、サイバーセキュリティ経営ガイドライン、デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」、政府機関等の統一基準群、CPSF、総務省のクラウドサービス関係ガイドライン、金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」、FISC 安全対策基準等の 9 文書を挙げている[11]。

それにもかかわらず経済産業省が SSDF 導入ガイダンスを策定する理由は、既存のガイドラインを廃止・置換するためではない。

既存ガイドラインは目的と対象が異なる

既存の国内ガイドラインには、経営管理を中心とするもの、情報システムの運用を中心とするもの、金融機関向けのもの、SBOM や OSS 管理に特化したものなどがある。そのため、企画、設計、開発、ビルド、テスト、リリース、脆弱性対応というライフサイクル全体を、一つの共通尺度で確認することは容易でない。

国際的な共通言語が必要である

海外政府や海外企業から「NIST SSDF のどのタスクに対応しているか」と問われた場合、日本独自のガイドラインに対応しているというだけでは、そのまま説明することができない。そこでガイダンス案は、国内ガイドラインと SSDF タスクとの対応関係を、**◎包含（ガイドライン該当章が SSDF タスクを含みより広い）、〇同等、△部分（タスクの一部のみ）、×該当なし**の 4 区分で整理し、その判断理由まで示すマッピングの見本を提示している。

もっとも、ガイダンス案は、マッピングは本来それぞれのガイドライン策定主体が自律分散的に行うことが望ましいとしており、今回示されたものはその先鞭にすぎない。今後、各ガイドラインの改訂に際して SSDF との整合が意識されることが見込まれる。

発注者と供給者の共通の物差しが必要である

政府や大企業が複数の供給者を比較する場合、それぞれが異なる基準を用いていると、セキュア開発の状況を横並びで評価できない。SSDF を共通軸とすれば、どのタスクを実施しているか、どの水準まで達成しているか、未実施事

---

[9] ガイダンス案は、NIST SP1800-44a 等を参考とした DevSecOps に基づくツール活用の基本モデルを示している。CI/CD パイプライン（コードの変更・ビルド・テスト・リリースを継続的かつ自動的に行う仕組み）に検査工程（コントロール・ゲート）を組み込み、セキュリティ要件を実行可能なコードとして定義する Security as Code（SaC）等により、開発の俊敏性とセキュリティの確実性を両立させることが想定されている。

[10] SBOM（Software Bill of Materials、ソフトウェア部品表）とは、ソフトウェアを構成するコンポーネント、そのバージョン、依存関係、提供元等を機械可読な形式で一覧化したものをいう。経済産業省は「ソフトウェア管理に向けた SBOM の導入に関する手引」Ver.2.0 を公表している。

[11] マッピングの対象は、経済産業省「SBOM 導入手引」Ver.1.0・Ver.2.0、Software-ISAC「情報システムにおけるセキュリティコントロールガイドライン」、デジタル庁「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」、経済産業省「サイバーセキュリティ経営ガイドライン」、NISC「政府機関等のサイバーセキュリティ対策のための統一基準群」、経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」、金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」及び FISC「金融機関等コンピュータシステムの安全対策基準・解説書」の 9 文書である。

項は何か、代替措置はあるか、どのような証拠があるかを、共通の形式で説明できるようになる。

したがって、今回のガイダンスは「ガイドラインをもう一つ増やす」というよりも、**既存の国内ガイドラインを横串で整理し、不足部分を補い、国際的な説明や調達に利用できる形に変換するためのメタ・ガイドライン**と理解するのが適切である。

9 NIST の SSDF をそのまま使わず、日本版ガイダンスを作る理由

NIST の SSDF は、幅広い業種・開発方法に利用できる反面、抽象度が高く、具体的な導入順序や達成水準までは詳細に示していない。そのため、企業の現場では、何から始めればよいか、現在の対応状況をどう確認するか、どの水準まで行えばよいか、未対応事項の優先順位をどう決めるか、どのような記録を残せばよいかが分かりにくいという問題がある。

そこでガイダンス案は、実証結果を踏まえ、SSDF に対して次の付加価値を与えることを目的としている。

- SSDF を組織・プロジェクトに導入する具体的な方法・手順（導入プロセス）
- 各タスクの達成の判断指針（達成レベル）と具体的な実践例
- タスクごとに利用可能なツールと適用の考え方・留意点
- タスクを実施しない場合に生じるリスクの明確化
- 国内ガイドラインとの対応関係及び不足事項の補完

10 アカウンタビリティベース・アプローチ

今回のガイダンス案で特に重要なのが、**アカウンタビリティベース・アプローチ**である。医療機器、重要インフラのシステム、一般消費者向けアプリケーション、社内の小規模な業務ツールでは、想定される被害や必要な安全水準が異なり、すべての企業、製品及びシステムに同じ対策を一律に求めることは現実的ではない。

そこでガイダンス案は、企業が自らリスクと目標を踏まえて対応水準を決定する一方、その判断について説明責任を負うという考え方を採用している。具体的には、①対象ソフトウェアと利用環境を明確にし、②想定されるリスクと必要な安全水準を分析し、③実施する対策と達成目標を決定し、④実施状況と証拠を記録し、⑤実施しない項目又は低い水準を選んだ場合にはその理由を説明し、⑥対策後も残るリスクを把握して適切な権限者が判断する、という流れである。

要するに、**対策を各社が合理的に選択する余地を認める代わりに、その選択が妥当であることを説明させる**という考え方である。

リスクベース・アプローチの発展形として位置付けられている

ガイダンス案は、この考え方を、従来のリスクベース・アプローチ及びベースライン・アプローチの課題を解消する発展形として明示的に位置付けている。リスクと対策効果の関係を定量的に評価することは困難であり、リスク量に基づいて対策の程度を決めることは難しい。他方、固定的・一律の基準を定めることも、対象によってリスクや要求水準が大きく異なる以上、適当でない。そこで、**リスク量ではなく「説明責任を果たせるか」という観点から対策を選択する**という発想が採られている。

その理論的基礎として挙げられているのは、会計基準における原則主義アプローチの**「Comply or Explain」**の考え方と、機能安全分野の**アシュアランス・ケース**である[12]。コーポレートガバナンス・コードにおける Comply or Explain と発想を同じくするものであり、法務・内部監査部門にとっては馴染みやすい枠組みといえる。

[12] ガイダンス案は、アカウンタビリティベース・アプローチの基礎として、会計基準における原則主義アプローチ（Principle-based Approach）の“Comply or Explain”の考え方と、機能安全・自動車サイバーセキュリティ（ISO/SAE 21434 等）の分野で用いられるアシュアランス・ケース（満たすべき主張について証拠と論証により妥当性を説明する文書）を挙げている。

11 「実施した」と言うだけでは足りない ― 証拠と残留リスク

アカウンタビリティを果たすためには、単にチェックリスト上で「対応済み」と回答するだけでは足りない。ガイダンス案は、実施した内容が妥当である理由を説明するとともに、**事後的にでも確認（検証）可能な文書**を残すこと、必要に応じて実施事項の入出力や活動記録等の客観的なデータをエビデンスとして保存することを求めている。

具体的には、例えば次のような証拠を保存することが重要となる。

- セキュリティ要件を定めた文書、役割・責任を定めた規程
- 設計レビュー及びコードレビューの記録
- 静的・動的テストの結果
- OSS や第三者製部品の一覧及び SBOM
- 脆弱性の評価・修正履歴
- 開発環境へのアクセス記録、教育・訓練の実施記録
- リリース承認の記録、経営層又は権限者による残留リスクの承認記録

最高レベルを達成してもリスクはゼロにならない

あわせて留意すべきは、ガイダンス案が、SSDF のタスクを網羅的に実施し最高の達成レベルを満たしたとしても、リスクがゼロになることは保証されないと明示している点である。静的検査・動的検査・構成解析のいずれの技術も完全性が保証されているわけではなく、完全性を高めようとすればコストは急速に増大するため、便益・リスク・コストを総合して判断することが必要とされる。

したがって、達成度を可視化することの意義は、安全性を証明することにあるのではなく、**対象ソフトウェアのセキュリティ水準と残留リスクを可視化し、権限者の判断に付すること**にある。この点は、取締役会・監査役への報告の在り方を検討する上で重要である。

12 導入は 7 つのステップで進める

ガイダンス案は、SSDF の導入プロセスを次の 7 段階に整理している。

ステップ	内容
①要求分析	対象となるソフトウェア、利用環境、重要性、想定される被害等を確認し、必要なセキュリティ水準を定める。委託開発、パッケージソフトウェア、OSS 及び外部コンポーネントも対象となり得る
②現状把握	現在どの SSDF タスクを実施しているかを確認する。既存の国内ガイドライン、社内規程、開発標準、テスト手順等への対応状況も活用する
③達成レベルの定義とギャップ分析	目標とする水準と現状を比較し、タスクごとに目標レベル・現状レベル・採用レベル・判断理由・未達事項への対応方針を整理する
④タスクの実践	組織体制、開発環境、アクセス管理、コード管理、テスト、第三者製部品の管理、脆弱性対応等を実施する（PO→PS→PW→RV の順序が基本）
⑤達成度評価	チェックリストと証拠資料に基づき、目標とした水準をどの程度達成しているかを評価する
⑥自己適合宣言の作成	必要に応じて、対象製品、対象範囲、達成したタスク、未達事項及び改善計画を明確にした上で、SSDF に沿った開発を行っていることを表明する
⑦ステップアップサイクルの推進	③に戻り、段階的な目標設定を選択して④⑤のサイクルを回し、最終的な目標レベルに到達する

なお改訂版では、**ツール導入プロセスは主にステップ④で実施されることが想定されるが、組織や開発現場によってはステップ②や⑤とも関連する**ことが明記され、ツール導入方法の実施は組織に合わせてカスタマイズを検討することが必要になる場合がある旨が追記された。これは、第 17 回タスクフォースの意見を踏まえた修正である。

13 3 段階の達成レベル、網羅率とスモールスタート

ガイダンス案では、各タスクの達成状況を、原則として 3 段階で示している。

レベル	基本的なイメージ
レベル 1	最低限の対応を実施しているが、部分的又は属人的な部分が残る
レベル 2	主要な事項が、組織的・標準的なプロセスとして実施されている
レベル 3	対策が高度に体系化され、測定、改善及び最適化まで行われている

もっとも、本年度の検討事項としては、**この段階数を 3 段階から 2 段階（最小限／標準以上等）に見直すこと**が挙げられていた。レベル 3 の難度が高いことにより導入のハードルが上がる可能性が指摘されていたためである。しかし、実証の結果、3 段階の達成レベルの識別が必要であると整理され、段階数は維持された。その上で、レベル 3 がすべての分野で必須ではなく、過度な要求と誤解されないよう位置付けを明確にする旨がガイダンスに盛り込まれている。

分野に応じた期待レベル

改訂版は、実証の対象とした分野ごとに、タスクごとに期待される達成レベルの目安を示している[13]。IT／標準分野については中小 IT 企業を含めて最低限期待される水準が、金融分野については都市銀行など要求水準が高い業種で期待される水準が整理されている。金融機関及びその委託先においては、標準的な分野より高い水準が期待され得る点に留意が必要である。

中間目標によるスモールスタート

第 17 回タスクフォースにおいて、組織のリソース制約を考慮し、完璧な実装を求めず、スモールスタートを可能とする最低限のレベル設定を検討すべきとの意見が示された。これを受け、改訂版では、**最終的に達成するレベルに対して達成時期を定め、その中間段階で、最終達成レベルから 1 段階低い中間目標を設定して段階的に水準を引き上げる方法**が追記された。

見落とされやすい「網羅率」という第二の軸

あわせて重要なのが、達成度は**タスクの網羅率**と**各タスクの達成レベル**の組合せによって決まるという整理である。ガイダンス案は、網羅率 50%、80%、100%という段階を示し、最初からすべてのタスクを網羅することは難しいため、段階的に範囲を広げることを想定している。

その上で、**網羅率 100%は必須ではない**と明示されている。CISA の自己適合宣誓様式[14]においても SSDF のすべてのタスクが求められているわけではないため、要件化されるタスクや優先度の高いタスクを選択し、必要に応じて網羅率を高めることが期待されるとされている。

重要なのは、単純に高いレベルを選択することではなく、**対象ソフトウェアのリスクに照らして、なぜそのレベル及び範囲を選択したのかを合理的に説明できること**である。

14 達成度評価とチェックリストの使い方

達成度評価は、①ガイダンス付録に示されるタスク達成レベルのチェックリストと比較する方法、②NIST SP800-218 のタスクの記述に対して実施内容が妥当であることの理由を説明する方法の 2 通りが想定されている。評価主体は、厳格さの必要性とコストに応じて、**供給者自身による第一者診断、発注者等による第二者診断、独立組織による第三者診断**から選択する。

---

[13] 分野別の期待レベルは、実証の対象を限定した上で整理されたものであり、IT／標準分野は中小 IT 企業を含めて最低限期待される水準、金融分野は都市銀行など要求水準が高い業種で期待される水準とされている。また、これらは適宜見直しが必要なリビングドキュメントと位置付けられている。

[14] 米国では、OMB 覚書 M-22-18 及びこれを更新する M-23-16 に基づき、CISA が公表した自己適合宣誓様式（Secure Software Development Attestation Common Form）による宣誓書の提出が求められている。

チェックリスト（改訂版では、タスク達成レベルの具体例をベースに、チェックしやすいフラットな構造に整理された）の使い方としては、次の 2 通りが示されている。

- **達成レベルの判定（必須要件・AND 要件）**：選択したレベルの項目をすべて満たした場合に当該レベルへの適合を宣言する。一部の弱点も許容できない場合に、特定のレベルを一通りクリアしていることを要件化する用法である
- **達成状況のスコアリング・可視化（任意要件・OR 要件）**：レベルごとの対応に制約を設けず、レベルに応じた重み付けにより総合スコアを算出し、業界ベンチマークとの比較や時系列での改善を可視化する用法である

さらにサマリーシートでは、分野ごとに求められる達成レベルに対する**実施率（要求比）**が示されるとともに、**タスクを実施しないことのリスクが高く、実施率が低いタスクを優先する**という考え方に基づき、対策の優先度が 3 段階（高・中・低）で提示される。限られた投資をどこに配分するかという経営判断に直接用いることができる情報である。

また改訂版では、タスク単位のリスクは情報量が多いという意見を踏まえ、**プラクティス単位でのリスク要点一覧**が新たに作成された。取締役会・監査役への説明資料としては、この一覧を出発点とすることが実務的である。

15 ツールの活用と 3 つの導入パターン

ガイダンス案は、セキュア開発を人手のみで実施するのではなく、ツールを活用して効率化することを重視している。想定されるツールとしては、ソースコード管理ツール、CI/CD ツール、環境構成管理ツール、コード署名・ハッシュ値生成ツール、SCA・SBOM 生成／管理ツール、OSS 脆弱性スキャンツール、静的コード解析ツール、動的検証ツール、要件・課題管理／トレーサビリティ管理ツール、ネットワーク監視ツール等が挙げられている。

もっとも、すべての企業に高度な統合ツール環境を求めるものではなく、導入済ツールの状況、組織のリソース・技術力、初期導入コスト、ガバナンス確保等の観点から、次の 3 つの導入パターンが示されている。

導入パターン	内容
(1)最小限ツール導入型	タスクに適合する単体ツールを最小限導入する。ソフトウェア構成管理、コード署名、SCA／SBOM 生成、静的コード解析等が該当する
(2)ツール拡充型	既存ツールに加えて複数のツールを組み合わせ、対象範囲を拡充する。SBOM 管理、動的検証、ネットワーク監視等が該当する
(3)ツールチェーン統合管理型	CI/CD 及び環境構成管理を中心に、開発工程全体を統合・自動化する。ツールチェーンの導入・運用・保守、ツールの設定、開発基盤の分離・保護等が該当する

改訂版では、第 17 回タスクフォースの意見を踏まえ、**脆弱性情報の収集と分析（RV.2.1）に対応するツールカテゴリとして、SBOM 管理ツールに加えて動的検証ツール及び OSS 脆弱性スキャンツールが追記**された。また、統合管理ツールの利用イメージを具体化するため、Ansible の Playbook 及び Dockerfile に関する説明が追記されている。他方、個別製品名やサポート状況等の情報については、短期間で陳腐化しやすく国のガイダンスに記載することは困難であるとして、現状の範囲にとどめられた。

16 第 17 回タスクフォースにおける意見と改訂内容（12 件）

今回の改訂版は、第 17 回タスクフォースにおいて受領した 12 件の意見[15]を踏まえたものである。意見の内訳は、①導入プロセスとタスクの記述 5 件、②ツール情報等の整理 4 件、③チェックリスト 2 件、④対象読者 1 件であり、それぞれに対する修正内容と考え方が参考資料 1 に整理されている。実務担当者にとっては、**どの論点が反映され、どの論点が「今後の検討課題」として留保されたかを把握しておくことが、次年度以降の改訂の見通しを立てる上で有用**である。

[15] 第 17 回タスクフォース（令和 8 年 1 月 22 日開催）における委員等の意見であり、行政手続法上の意見公募手続（パブリックコメント）とは異なる。意見の内容及びこれに対する修正内容は、参考資料 1 に一覧として整理されている。

No.	意見の要旨	区分	改訂版における対応
1	RV.2.1（脆弱性情報の収集と分析）に対応するツールカテゴリに、SBOM 管理ツール以外に脆弱性データベース検索ツール等も含めるべき	ツール情報	**反映。**表 5-7 の RV.2.1 に動的検証ツール及び OSS 脆弱性スキャンツールを追記し、付録 9.1 にも概要を記載
2	自己適合チェックを簡易に実施できるウェブサイトを整備してほしい	チェックリスト	**見送り。**予算及びアクセス制御への留意が必要であるとして今後の検討課題とされた
3	リスク低減効果の記載が巨大なインシデントに偏っており、より身近なインシデントを紹介すべき	導入プロセス・タスクの記述	**現状維持。**全タスクについてリスクを一般化した内容と併せて提示しているとされた
4	チェックリストにシステムインフラの構築を想定した項目を追加すべき	チェックリスト	**現状維持。**項目の肥大化を避けるため要点を絞る方針とされ、今後の検討課題とされた
5	「ツールコスト効果」シートについて、前提知識の有無による工数等を区別して示すべき	ツール情報	**現状維持。**標準的な参考値にとどめ、細分化は今後の検討課題とされた
6	「タスク俯瞰マップ」の遂行主体「技術者」をより細かく区分すべき	導入プロセス・タスクの記述	**反映。**表 8-1 の遂行主体を「ソフトウェア技術者」「インフラ構築者」「セキュリティ技術者」に再定義
7	Ansible のプレイブック、Dockerfile のベストプラクティス、CIS ベンチマーク等を参考情報として記載すべき	ツール情報	**反映。**8.1.9(5)に Ansible の Playbook を例示し、9.1 に Playbook 及び Dockerfile の説明を追記
8	リソース制約を考慮し、スモールスタートのための最低限のレベルを設定すべき	導入プロセス・タスクの記述	**反映。**5.2.7 に、目標レベルより 1 段階低い中間目標を設定してステップアップする方法を追記
9	ツールの利用条件、OSS のサポート状況、組合せ例等の製品情報を追記すべき	ツール情報	**見送り。**個別製品名や短期間で陳腐化しやすい情報を国のガイダンスに記載することは困難とされた
10	タスク単位のリスクは情報量が多いため、プラクティス単位で整理した一覧が必要	導入プロセス・タスクの記述	**反映。**10.2 にプラクティス単位のリスク要点一覧（表 10-1）を新規に作成
11	「ツール導入プロセス」はステップ 4 以外（ステップ 2、5 等）とも関連する	導入プロセス・タスクの記述	**反映。**5.1 に、ステップ 2、5 等とも関連し、組織に合わせたカスタマイズの検討が必要となる場合がある旨を追記
12	対象読者として、具体的な想定読者や組織を指定すべき	対象読者	**反映。**表 8-1 にタスクごとの主な読者（組織レベル・組織内担当者レベル）を記載し、1.3 から参照

12 件のうち 7 件が改訂版に反映され、5 件は現状維持又は今後の検討課題とされた。留保された論点（ウェブ上の自己診断ツールの整備、チェックリスト項目の拡充、コスト情報の精緻化、製品情報の充実）は、いずれも実務における使い勝手に直結する事項であり、来年度以降の取組として示されている**代表分野に対応した応用編・中小企業向けの簡潔版の作成、業界団体との連携による普及促進、コスト負担の在り方の検討**の中で扱われる可能性がある。

17 政府調達との関係 ― 日本ではどの段階にあるのか

経済産業省は、SSDF を実践するための国内事業者向け文書を策定し、自己適合宣言の仕組みや政府調達等での活用を通じて実効性を高め、QUAD 共通原則[16]を履行することを政策上の目標として掲げている。

もっとも、我が国において、現時点で SSDF への適合や自己適合宣言が全省庁共通の政府調達要件として義務化されたわけではない。令和 8 年度の検討では、**米国における大統領令の改訂を踏まえ、自己適合宣言の仕組み・政府調達等での要件化ではなく、まず第三者による管理・運用を伴わない国内事業者向けの自己チェックリストを作成する**こととされ、政府調達における具体的な活用方法については、米国の政策動向等も踏まえて今後検討することとさ

[16] QUAD（日米豪印）のサイバーセキュリティ・パートナーシップに基づく「安全なソフトウェアに関する共同原則」をいい、政府調達ソフトウェア等について安全なソフトウェア開発手法の実践に準拠することを目指す旨が合意されている。

れている。

したがって、我が国における現在の位置付けは、**直ちに企業を法的に拘束する基準ではないが、将来の政府調達や重要分野のベンダー管理に利用することを見据えた制度形成段階**にあると評価できる。第三者認証制度の導入も、現時点では予定されていない。

18 既存の国内ガイドラインでは不足しやすい事項

ガイダンス案は、既存の国内ガイドラインでは十分に対応されていないタスクについて、NIST SP800-218 の Reference を参照しつつ、対策の考え方・重要性及び具体策を補足している。特に不足しやすいものとして、次の 10 タスクが挙げられている（★はガイダンス案が「上級者向け」と位置付けたもの）。

タスク	内容
PO.3.1	ツールチェーンに含めるツールの決定
PO.3.2	ツール及びツールチェーンの導入・運用・保守
PW.4.2★	安全性の高い自社製コンポーネントの作成
PW.6.1	実行ファイルのセキュリティを高めるツールの利用
PW.6.2	コンパイラ・ビルドツール等の設定の決定及び実施
PW.7.2	セキュアコーディング基準に従ったコードレビュー・コード解析の実施
PW.8.1	動的テスト方法の決定
PW.8.2	動的テストの設計及び実施
RV.3.2★	根本原因を長期的に分析することによるパターンの特定
RV.3.3	類似の脆弱性の積極的な検出

これらは、完成後の脆弱性診断だけでは対応できない、開発・ビルド・供給プロセス全体の安全性に関する事項である。既存のガイドライン対応をもって足りると考えている企業ほど、この領域に空白が生じやすい。

19 脆弱性を修正して終わりではない

SSDF の RV（脆弱性への対応）では、発見された脆弱性を個別に修正するだけでなく、なぜその脆弱性が作り込まれたのかを分析し、同じ原因による問題を減らすことが重視されている。具体的には、次の対応である。

- 脆弱性の直接的・根本的な原因を調査する
- 同様の原因による脆弱性が他にないか確認する
- 他の製品やシステムにも横展開して調査する
- 設計基準、開発ルール、教育、ツール設定等を見直す
- 同種の問題が減少したかを継続的に評価する

これは、個別のインシデント対応を、開発プロセス全体の品質改善につなげる考え方であり、単なる脆弱性管理を超えて、**内部統制上の是正措置（再発防止）と同じ構造**を有する。

20 企業実務に与える影響

以下は、ガイダンス案の内容から導かれる企業法務・ガバナンス上の実務的な示唆である。現時点で SSDF に対応していないことが、直ちに法令違反となるわけではない。しかし今後、政府、金融機関、重要インフラ事業者、大企業等のソフトウェア調達において、次の事項が契約やベンダー審査の対象になる可能性がある。

- 適用する SSDF タスクと達成水準（分野に応じた期待レベルを含む）

- 開発・ビルド環境の保護、ソースコードへのアクセス管理
- OSS・第三者製コンポーネントの管理及び SBOM の作成・提供
- コードレビュー、静的解析及び動的テストの実施と記録
- 脆弱性の通知期限及び修正期限、再委託先へのセキュリティ要求
- 開発・テスト・修正記録の保存並びに発注者による監査権
- 未達事項に関する改善計画及び自己適合宣言の内容の正確性

特に、企業が「SSDF 準拠」「安全な開発体制を整備済み」などと対外的に説明する場合には、説明の対象範囲と裏付けを明確にする必要がある。対象会社、対象製品、バージョン、対象期間、適用タスク、適用除外、未達事項、前提条件及び証拠資料を曖昧にしたまま広範な表現を用いると、事故発生時に、その説明と実態の不一致が問題となり得る。

具体的には、契約上の表明保証違反、調達先への不正確な説明、損害賠償責任、入札・調達資格上の問題、取締役の善管注意義務及びレピュテーションの低下が問題となり得る。

21 取締役・監査役・内部監査部門が確認すべき事項

SSDF 対応を開発部門のみに委ねるべきではない。経営者、取締役、監査役及び内部監査部門は、少なくとも次の事項を確認する必要がある。

No.	確認項目	確認のポイント
1	重要ソフトウェアを把握しているか	自社が開発・提供・利用するソフトウェアのうち影響の大きいものを特定し、その外部委託先・部品供給者を把握しているか
2	責任体制が明確か	セキュア開発に関する責任者と、調達・開発・品質保証・法務・内部監査の役割分担が明確か。責任主体と遂行主体の区別を意識しているか
3	開発基盤が保護されているか	開発・ビルド・リリース環境の分離、アクセス管理、コード署名等により、正規の工程への侵害を防止しているか
4	OSS・第三者製部品を管理しているか	SBOM 等により構成部品を把握し、脆弱性情報を継続的に監視しているか
5	検証結果が記録されているか	設計レビュー、コードレビュー、静的・動的テストの結果が、事後的に検証可能な形で保存されているか
6	達成レベルと範囲の選択理由を説明できるか	対象システムごとに、なぜその達成レベル及び網羅率を選択したのかを、リスクとコストの観点から説明できるか
7	残留リスクが経営に報告されているか	重大な未達事項及び残留リスクが、対策の優先度とともに経営層・取締役会に報告されているか
8	委託先・再委託先に要求が伝わっているか	契約上、必要なセキュリティ要求、記録保存義務及び監査権が確保されているか
9	根本原因分析と横展開を行っているか	脆弱性の受付・評価・通知・修正のみならず、根本原因の分析、類似脆弱性の横断調査及び開発プロセスの見直しに反映しているか
10	対外的な説明が実態に裏付けられているか	「準拠」「安全性」に関する対外的な説明が、実態と証拠に裏付けられているか。誇張した表示となっていないか

22 企業が当面着手すべきこと

すべての企業が、直ちに SSDF の全タスクへ全面的に対応する必要はない。網羅率 100%が必須ではないことは前記のとおりである。まずは、次の順序で着手することが現実的である。

① 対象を絞る

自社が開発又は提供するソフトウェアのうち、顧客、社会、事業継続への影響が大きいものを特定する。

② 既存の対応を棚卸しする

社内規程、開発標準、テスト、アクセス管理、OSS 管理、SBOM、脆弱性対応等を、SSDF のタスクに対応付ける。国内ガイドラインへの対応実績は、そのまま活用できる場合が多い。

③ 不足事項を把握し、中間目標を設定する

特に、開発環境、ビルド工程、ツールチェーン、リリースの完全性、第三者製部品及びリリース後の脆弱性対応を確認する。その上で、分野に応じた期待レベルを参照しつつ、当面は 1 段階低い中間目標を設定し、優先度の高いタスクから網羅率を高める。

④ 証拠を残す

対策を実施するだけでなく、レビュー記録、テスト結果、ログ、修正履歴、承認記録等を保存する。

⑤ 経営判断につなげる

未達事項、対応コスト、残留リスク及び対応期限を整理し、重要なものを経営会議又は取締役会に報告する。

23 おわりに

経済産業省の SSDF 導入ガイダンス案は、単なる「安全なプログラムの書き方」を示す文書ではない。その本質は、**ソフトウェアの開発、調達、リリース及び脆弱性対応について、企業が合理的な管理体制を構築し、その判断と実施状況を証拠に基づいて説明するためのガバナンス・フレームワーク**にある。

国内に多数のガイドラインが存在する中で、このガイダンスが目指しているのは、既存の基準をすべて置き換えることではない。既存の取組を SSDF という国際的な共通軸で整理し、不足する部分を補い、供給者と発注者が共通の言葉で安全な開発について説明・確認できるようにすることである。

今回の改訂により、達成レベルは 3 段階が維持される一方、中間目標の設定や網羅率の段階的な引上げが明示され、スモールスタートの道筋が具体化された。制度設計としても、当面は自己適合宣言や政府調達での要件化ではなく、事業者が自主的に用いる自己チェックリストを整備する方向が示されている。義務化を待つのではなく、自主的な整理を先行させることが可能な段階にあるといえる。

SSDF への対応は、チェックリストを埋めること自体が目的ではない。**「事故が起きなかったから安全だった」ではなく、「事故を防ぐために合理的な仕組みを設け、それを実際に運用していた」と説明できる企業になること**が、最終的な目的である。

理解度チェック（〇×問題 10 問）

【問題】次の記述は正しいか（〇×）。

Q1　SSDF は、企業に対して特定の開発ツール又は開発手法への変更を求めるフレームワークである。

Q2　SSDF の実践領域は、PO（組織の準備）、PS（ソフトウェアの保護）、PW（セキュアな開発）、RV（脆弱性への対応）の 4 つで構成される。

Q3　SolarWinds 事件は、正規の供給者による正規の更新プログラムを通じて侵害が生じ得ることを示した事案である。

Q4　今回の改訂により、タスクの達成レベルは 3 段階から 2 段階に変更された。

Q5　アカウンタビリティベース・アプローチは、会計基準における原則主義（Comply or Explain）の考え方を採り入れたものである。

Q6　改訂版では、最終的な目標レベルより 1 段階低い中間目標を設定してステップアップする方法が追記された。

Q7　自己適合宣言を行うためには、SSDF のすべてのタスクを実施し、網羅率 100%を達成することが必須である。

Q8　達成度評価は、供給者自身による第一者診断のほか、発注者による第二者診断、独立組織による第三者診断が想定されている。

Q9　我が国では、現時点で、SSDF への適合が全省庁共通の政府調達要件として義務化されている。

Q10　SSDF のタスクを網羅的に実施し最高の達成レベルを満たせば、リスクはゼロになると整理されている。

【解答】Q1×（何を達成すべきかを示すものであり、開発方法の変更を求めるものではない） Q2〇　Q3〇　Q4×（実証の結果、3 段階が維持された） Q5〇　Q6〇　Q7×（網羅率 100%は必須ではない） Q8〇　Q9×（現時点で義務化されていない） Q10×（残留リスクは存在するとされている）

以　上