

バイデン政権、サイバーセキュリティ戦略において大幅な方向転換を提案

—「脆弱でリスクの高い」ソフトウェア開発者には責任を課す方向へ

ブライアン・E・フィンチ、エイミー・P・ゴーシュ、アリエル・R・ヘフェズ

- 本戦略は、ソフトウェア開発者の負う法的責任について、サイバーセキュリティ市場の根本的な変更もたらず提案をしています。
- 提案されている法律は、ソフトウェア開発者が独自の責任を限定する手段を制限し、他方で、新たなセーフハーバープログラムを通じて、ソフトウェア開発者に一定の基準を満たすインセンティブを与えることを目的としています。
- 連邦調達規則におけるソフトウェアセキュリティの責任強化の推進など、議会の承認を要さないものからこの提案の則った対応を始める可能性があるため、企業はこれに備える必要があります。

2023年3月2日、バイデン政権は、[国家サイバーセキュリティ戦略](#) (National Cyber Security Strategy) を公表し、サイバー攻撃への防御力がより高く、回復力があり、価値観の一貫したデジタルエコシステムを構築する意図を発表しました。この戦略には、脆弱性のあるシステムを作ったソフトウェア企業に、責任を負わせるという政権の優先的な取り組みが含まれています。この『戦略』は次の5つの中核となる目的に基づいています。1) 重要なインフラストラクチャの防衛、2) サイバー攻撃脅威要因の崩壊、3) 安全性と強靱性を推進するための市場原理の形成、4) 強靱性のある未来へのサイバー環境への投資、そして 5) 共通の目標を追求するための国際パートナーシップの構築、を目指します。特に第3の目的は、セキュリティソフト開発者が、性能の劣るソフトウェアセキュリティに対する責任を契約上否認できないようにすることに重点を置いています。これにより、ソフトウェア製品やサービスの開発メーカーは、セキュリティが不十分なソフトの開発やメンテナンス作業に対して責任を負わせられる可能性が高まります。

この方向転換を正当化する上で、バイデン政権は、「コア経済的および国家安全保障上の利益を優先するために業界を動かす」には市場の力が不十分であったと指摘しています。さらに、ソフトウェアメーカーは契約により免責できるので、「セキュア・バイ・デザイン原則の遵守やリリース前のテスト実施等のセキュリティ対策の強化へインセンティブが低下」とも述べてきます。この現状を打破するために、バイデン政権は、ソフトウェア開発者が「消費者、企業、または重要インフラ事業者に対して負うべき相当の注意義務を果たせなかった場合、かかるソフトウェア開発者は責任を負わなければならない」と考えています。

法律が未整備なため、メーカー側に契約を利用した抜け道があるなど、責任の主体が不明確であり、そこにアンバランスが生じています。そこで、バイデン政権はソフトウェア製品およびサービスに対する責任を確立するための新しい法律を提案し、この現状を解消しようと試みています。ホワイトハウスからの説明によると、その法案は、ソフトウェア開発者が契約を利用してエンドユーザーに責任を転嫁することを禁止し、特定の高いリスクを伴う状況で用いられるソフ

トウェアについては、より厳しい基準の適用を提案しています。この『戦略』は、新たな政策の最終目標について次のように述べています。責任の主体を、「脆弱性のあるソフトウェアを使用し、その結果被害を被ったエンドユーザーや、製品の一部を構成するソフトウェアコンポーネントのオープンソースソフトウェア開発者にするのではなく、それらのコンポーネント等を統合し、最終製品を開発したソフトウェアメーカーとすることです。なぜなら、最終的な開発メーカーが最もソフトウェアの脆弱性から生じる悪影響を想定し、予防措置をとるための手段を講じることができる立場にあるからです」。

同『戦略』によると、ソフトウェア開発者に責任を課すこの法案は、ソフトウェア製品やサービスを安全に開発・維持するプロバイダーを保護する「順応性の高いセーフハーバーフレームワーク」と組み合わせられます。この提案は、裁判所による法の執行を通じて強制される事実上のセキュリティ基準を課すことになり、所定の基準を満たす企業は法的保護を受け、満たさない企業に対しては脆弱なソフトウェア開発、パッチングや脆弱性の修復における過失、その他の請求原因による訴えのリスクを高めることになると考えられます。同『戦略』には、この法案の更なる詳細は記載されていませんが、政権は議会および民間部門と協力して法案を作成する意向です。

具体的な法の条文はまだ提案されておらず、このようなイニシアチブが大きな修正なしに議会を通過するという保証はないものの、同『戦略』の法的責任に関する提案は、ソフトウェア市場の根本的な変化を意味します。この法律が制定されれば、既存の州レベルの法的責任の枠組みを大きく先取りし、裁判所がソフトウェア開発者のパフォーマンスを比較できる合意された「基準」を確立することになると考えられます。

従って、政権の提案は議会で多くの議論を呼ぶことになるでしょう。その間、バイデン政権はこの目標に向けて準備を進め、連邦調達規則におけるソフトウェアセキュリティの責任強化の推進など、議会の意見を要さないものから最初の措置を講じられる可能性があるため、企業はこれに備える必要があります。また、SECなどの規制当局が、脆弱性の高いソフトウェアの開発者に対して行う強制捜査についても、政権は好意的に受け止められると思われれます。

また、脆弱なソフトウェア開発に関連する不法行為責任を懸念する企業は、SAFETY Act を通じた法的保護を受けることができます。SAFETY Act は、サイバーセキュリティツールを含む「テロ行為」を抑止するために展開される様々なセキュリティ製品やサービスに対する第三者の不法行為責任を制限または排除する既存のセーフハーバープログラムです。企業はこれらの保護を早急に追求することで、新しいセーフハーバー制度が確立される前から責任保護の適用を受けることができます。

本稿の原文(英文)につきましては、[New Biden Administration Cyber Strategy Proposes Dramatic Shift in Order to Hold Software Developers Liable for “Insecure” Software](#) をご参照ください。

本稿の内容に関する連絡先

ジェフ・シュレップファー（日本語対応可）

jeff.schrepfer@pillsburylaw.com

サイモン・バレット

simon.barrett@pillsburylaw.com

松下 オリビア（日本語対応可）

olivia.matsushita@pillsburylaw.com

奈良房永（日本語版監修）

fusae.nara@pillsburylaw.com

Brian E. Finch

brian.finch@pillsburylaw.com

Aimee P. Ghosh

aimee.ghosh@pillsburylaw.com

Arielle R. Heffez

arielle.heffez@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

田中里美

satomi.tanaka@pillsburylaw.com

This publication is issued periodically to keep Pillsbury Winthrop Shaw Pittman LLP clients and other interested parties informed of current legal developments that may affect or otherwise be of interest to them. The comments contained herein do not constitute legal opinion and should not be regarded as a substitute for legal advice.

© 2023 Pillsbury Winthrop Shaw Pittman LLP. All Rights Reserved.