Legal Wire

pillsbury

Japan Practice

Vol. 112 / June 2021

バイデン大統領、広範囲にわたる新たなサイバーセキュリティ改革を発表

ブライアン・E・フィンチ、クレイグ・J・サパースタイン、ローズ・フォウラー・ラップ

- 2021 年 5 月 12 日、バイデン大統領は、国家サイバーセキュリティの向上に関する大統領令を発表し、連邦政府のサイバーセキュリティの最新化を目的とする広範囲な改革を提案しました。今回の発表は、最近頻発しているサイバー攻撃やランサムウェアに関し、連邦政府のみならず、政府調達契約に基づいて連邦政府に納入する業者のサイバーセキュリティを強化することを目的としています。
- この大統領令には、ゼロトラスト・アーキテクチャ、エンドポイントでの検知及び対応、データの暗号化並びに多要素認証の更なる普及推進が含まれています。
- この大統領令は、重要なソフトウェアに対する新たなサイバーセキュリティ要件の策定を指示するとともに、必要なアップデートがなされない場合には、レガシーソフトウェアを削除することも義務付けています。

SolarWinds 社のサイバー攻撃及び Colonial Pipeline 社のランサムウェア事件を受けて、2021 年 5 月 12 日、バイデン大統領は、待望されていた「国家サイバーセキュリティの向上に関する大統領令」（Executive Order on Improving the Nation's Cybersecurity）を発表し、連邦政府の調達業者に対するサイバーセキュリティ要件の大幅な変更について、その概要を示しました。この大統領令では、とりわけ、ソフトウェアのサプライチェーンにおけるセキュリティの向上、サイバーセキュリティ安全審査委員会の設置、消費者向け表示プログラムの創設、ゼロトラスト・アーキテクチャ及び多要素認証の導入、そして、とりわけ、政府のネットワークに影響を与える可能性のある侵害（Breach）に関する情報の共有をプロバイダーに義務付けることが提案されています。以下では、大統領令の内容のうち、クライアントに特に関連するものについて、詳細な情報を紹介します。

脅威情報の共有を妨げる障害の除去

情報共有の妨げとなる現在の障害を除去するために、行政管理予算局（Office of Management and Budget）長は、国防長官、司法長官、国土安全保障長官及び国家情報長官と協力して、連邦調達規則（Federal Acquisition Regulation, FAR）及び国防省調達規則（Defense Federal Acquisition Regulation Supplement）の見直し及び勧告を行うことになります。今回の大統領令が、どのように、連邦政府との契約におけるサイバーセキュリティ要件を広範囲にわたって変更するよう指示し、政

府に「権限及びリソースを十分に発揮する」よう求めているかについては、こちらの政府契約についてのサイバーセキュリティ・ニュースレター（英語）をご覧ください。

ゼロトラスト・アーキテクチャ

この大統領令に含まれる最も重要な対策のひとつは、連邦政府全体に「ゼロトラスト・アーキテクチャ」（Zero Trust Architecture, ZTA）を導入するよう指示していることです。この大統領令では、ZTA を「あらゆる要素、ノード又はサービスに対する無条件の信頼を排除し、代わりに、アクセスやその他のシステム対応を決定するにあたって、複数のソースからのリアルタイム情報を介して運営状況を継続的に検証をすることを必要とする」システムと定義しています。これは、アクセス及び不正アクセスの拡大（ラテラル・ムーブメント）を制限し、異常又は不正な活動を探知し、「脅威が変化を続ける状況の中で、リアルタイムでデータ保護に集中するために、インフラのすべての側面を通して、包括的なセキュリティ監視、きめ細かなリスクベースのアクセス制御、そして、システムセキュリティの自動化を組み合わせて導入する」ものです。なお、大統領令は ZTA を支持していますが、他方で、指針となる ZTA がどのようなものなのかを特定していません。

大統領令は、各政府機関の長に対し、ZTA を実施するための計画を策定するよう求めています。各計画には、米国標準技術研究所（National Institute of Standards and Technology, NIST）が既に公表している移行手順を組み込む必要があり、既に完了している手順や、最も緊急性の高いセキュリティ上の影響を与える機能を、実施のスケジュールとともに記載する必要があります。

また、この大統領令には、クラウド技術に移行する政府機関が、その技術に特化した ZTA を採用することを求める要件も含んでいます。この移行を促進するために、サイバーセキュリティ・インフラセキュリティ庁（CISA）は、現行のサイバーセキュリティのプログラム、サービス及び性能を、ZTA を備えるクラウドコンピューティング環境に対応できるように更新します。また、CISA は、クラウドサービス事業者を規律するセキュリティ諸原則のガイダンスを策定するために、国土安全保障長官及び一般調達局長と協力して、FedRAMP プログラムを処理することになっています。

データ暗号化及び多要素認証

クラウドサービスのサイバーセキュリティを向上させることを目的とするもうひとつの施策は、各政府機関に対して、保存中及び転送中のデータに対して多要素認証と暗号化を導入することを義務付けるものです。連邦一般行政部（Federal Civilian Executive Branch）の長は、大統領令から 60 日後に、これらのセキュリティ対策の導入状況の報告を開始し、この報告は、暗号化及び認証の措置が完全に実施されるまで続けることになっています。CISA は、これらの措置を実施するための技術や手続の導入を促進するために、「あらゆる適切な措置」を講じることとされています。

サプライチェーンにおける重要なソフトウェアの保護

大統領令は、「重要なソフトウェア」を保護することの必要性を強調しています。重要なソフトウェアとは、一般的には、「信頼（Trust）（昇格したシステム特権やネットワーク及びコンピューティングリソースへの直接アクセスを許可又は要求するなど）に不可欠な機能を実行するソフトウェア」と定義されていますが、現在のところ、この用語が何を意味するかは明確ではありません。より具体的な定義は、NIST が、国家安全保障局（National Security Agency）、CISA、行政管理予算局及び国家情報長官室と協議の上で策定します。その後、CISA 及び NIST は、その定義をもとに、各政府機関が使用するソフトウェアのリストを作成します。この両機関は、最小特権、ネットワークセグメンテーショ

ン及び適切な設定方法について適用される重要なソフトウェアについてのガイドラインを発表する予定です。

大統領令から 1 年以内に、国土安全保障長官は、他の部門の長と協議の上、政府にソフトウェアを供給する企業が、これらの新しいサイバーセキュリティ要件を遵守することを義務付ける契約文言を連邦調達規則評議会（FAR 評議会）に提案します。その後、FAR 評議会はそれらの提案を検討し、連邦調達規則を修正します。サプライチェーンのうち、要件を満たさないソフトウェア製品はすべて排除されることになり、レガシーソフトウェアについても、この厳しい要件から免除されることはありません。

NIST は、新たなソフトウェア・サプライチェーンのセキュリティ要件及び基準を遵守するため、新しい基準、ツール及びベストプラクティスを策定するにあたり、連邦政府、民間企業及び学界から意見を募ります。

サイバーセキュリティの脆弱性及びインシデント検出の向上

大統領令には、連邦政府のネットワークにおけるサイバーセキュリティの脆弱性及びインシデント検出の向上を目的とするという項目が含まれており、政府はこの目標を達成するために「あらゆる適切なリソース及び権限を活用する」と規定しています。大統領令では、連邦一般行政部に属する政府機関が、エンドポイントでの検知及び対応（Endpoint Detection and Response, EDR）の導入を主導するよう求めており、これは、CISA が策定した要件を遵守することになります。EDR の実施を可能にするため、各政府機関にリソースが提供される予定です。また、その項目は、各政府機関に対して、CISA との間で、継続的な診断と脅威の軽減（Continuous Diagnostics and Mitigation, CDM）プログラムについて、覚書を作成又は更新し、CISA がオブジェクトレベルのデータをアクセスできるようにすることを求めています。

大統領令から 45 日以内に、国家安全保障局長官は、EDR アプローチに関し、及び、これらの手段は各政府機関が運用すべきか、それとも、中央集中化したサービスを通じて運用すべきかなどに関する勧告など、国家安全保障システムに影響を与えるサイバーインシデントの検知を向上させるための行動を勧告することになっています。

サイバーセキュリティ安全審査委員会

大統領令では、連邦公務員及び民間のサイバーセキュリティ企業やソフトウェアサプライヤーの担当者で構成されるサイバーセキュリティ安全審査委員会（Cybersecurity Safety Review Board）を設置します。サイバーセキュリティ安全審査委員会は、連邦一般行政部の情報システム又は非連邦システムに影響を与える「重大なサイバーインシデント」、脅威の活動、脆弱性、影響を最小限に抑える活動及び政府機関の対応をレビューし、評価します。

委員会の最初のレビューは、2020 年の年末に発生したサイバーインシデントに関するものです。委員会は、その後、サイバーセキュリティ及びインシデント対応の実務の改善や、委員会の構成及び運営に関連する決定についても勧告を行います。

FedRAMP の最新化

大統領令に含まれる FedRAMP の最新化に向けたステップの 1 つは、評価、認証、継続的な監視及びコンプライアンスを含む FedRAMP のライフサイクル全体を通して、自動化を組み入れることです。最新化のプロセスには、関連するコンプライアンスの枠組みを特定すること、及び、必要に応じて FedRAMP プロセスの該当箇所の代わりに使用することを認めることも含まれています。

締切日

脅威情報の共有を妨げる障害の除去

- 大統領令から 60 日以内に、行政管理予算局は、国防長官、司法長官、国土安全保障長官及び国家情報長官と協議の上、連邦調達規則及び国防省調達規則を見直し、サイバーセキュリティに関する契約文言の変更を提案します。
- 大統領令から 45 日以内に、国土安全保障長官は、国家安全保障局長官、司法長官及び行政管理予算局長と協議の上、報告義務に関する契約文言に関連するその他の提案を行います。
- 大統領令から 60 日以内に、CISA 長官は、国家安全保障局長官、行政管理予算局長及び一般調達局長と協議の上、現行の政府機関固有のサイバーセキュリティ要件を見直し、標準的な契約文言を FAR 評議会に提案します。
- 提案の受領後 60 日又は 90 日以内に、提案の種類に応じて、FAR 評議会は更新案を検討し、公表します。
- 大統領令から 120 日以内に、国土安全保障長官及び行政管理予算局長は、サービスプロバイダーが、必要に応じて関連機関、中央情報局(CIA)及び連邦捜査局(FBI)に対してデータを共有することを確実にするための適切な措置を講じます。
- 大統領令から 90 日以内に、国家安全保障局長官、司法長官、国土安全保障長官及び国家情報長官は、サイバーインシデントの報告が迅速かつ適切に共有されようにするための手順を共同で策定します。

連邦政府のサイバーセキュリティの最新化

- 大統領令から 60 日以内に、各政府機関の長は、①クラウド技術の導入及び利用のためのリソースを優先化するために、既存の政府機関の計画を更新し、②ZTA を実施するための計画を策定し、③これらの計画に関する報告書を行政管理予算局及び国家安全保障担当大統領補佐官に提出します。
- 大統領令から 90 日以内に、行政管理予算局、CISA 及び FedRAMP は、連邦クラウドセキュリティ戦略についてのガイダンスを策定し、提供します。
- 大統領令から 90 日以内に、行政管理予算局、CISA 及び FedRAMP は、連邦一般行政部のためのクラウドセキュリティ技術リファレンス・アーキテクチャ文書を発行します。
- 大統領令から 60 日以内に、CISA は、連邦一般行政部に属する政府機関のためのクラウドサービス・ガバナンス・フレームワークを策定し、発行します。

- 大統領令から 90 日以内に、連邦一般行政部に属する政府機関の長は、CISA と協力して、自部門の未分類データを評価し、その報告書を CISA 及び行政管理予算局に提出します。
- 大統領令から 180 日以内に、各政府機関は、多要素認証並びに保存中及び転送中のデータの暗号化を導入します。連邦一般行政部に属する政府機関の長は、この目標を達成するまで、60 日ごとに進捗報告を行わなければなりません。
- 大統領令から 90 日以内に、CISA 長官は、司法長官、連邦捜査局長官及び FedRAMP と協議の上、連邦一般行政部のクラウド技術に関連するサイバーセキュリティ及びインシデント対応活動を共同で行う枠組みを確立します。
- 大統領令から 60 日以内に、一般調達局長は FedRAMP の最新化を開始しなければなりません。

ソフトウェア・サプライチェーンのセキュリティ強化

- 大統領令から 30 日以内に、NIST は、新しい標準、ツール及びベストプラクティスを特定又は策定するための意見を募ります。大統領令から 180 日以内に、NIST は暫定ガイドラインを発表し、大統領令から 360 日以内に、追加ガイドラインを発表します。
- 暫定ガイドラインの発表から 90 日以内に、NIST はソフトウェア・サプライチェーンのセキュリティ強化に関するガイダンスを発行します。
- 大統領令から 60 日以内に、商務長官は、通信情報担当次官補及び電気通信情報局長官と連携して、ソフトウェア部品表の最低要件を公表します。
- 大統領令から 45 日以内に、NIST は、国家安全保障局長官、CISA 長官、行政管理予算局長及び国家情報長官と協力して、「重要なソフトウェア」の定義を公表します。
- その定義の発表から 30 日以内に、CISA 及び NIST は、その定義を満たすソフトウェア及びソフトウェア製品のカテゴリのリストを特定し、各政府機関に提供します。
- 大統領令から 60 日以内に、NIST 及び CISA は重要なソフトウェアのセキュリティ対策をまとめたガイダンスを発行します。
- そのガイダンスの発行から 30 日以内に、行政管理予算局は各政府機関に遵守を求めるための適切な措置を講じます。
- 大統領令から 1 年以内に、国土安全保障長官は、国防長官、司法長官及び行政管理予算局と協議の上、ソフトウェアの供給者に対して要件を遵守することを求める契約文言を FAR 評議会に提案し、その後、評議会は FAR を検討し、修正します。
- 大統領令から 60 日以内に、NIST 及び国家安全保障局は、ベンダーがソフトウェアのソースコードをテストするための最低基準を推奨するガイドラインを発表します。
- 大統領令から 270 日以内に、NIST 及び連邦取引委員会（FTC）は、消費者向け表示プログラムの基準を特定します。
- 大統領令から 1 年以内に、NIST は、消費者向け表示プログラムの試行につき見直しを行います。
- 大統領令から 1 年以内に、商務長官は、進捗状況を検討し、ソフトウェアのサプライチェーンの安全性を確保するために必要な追加措置を説明した報告書を大統領に提出します。

サイバーセキュリティ安全審査委員会の設置

- サイバーセキュリティ安全審査委員会は、設立後 90 日以内に、サイバーセキュリティ及びインシデント対応の実務を改善するための勧告を国土安全保障長官に提供します。
- 委員会の最初のレビューから 30 日以内に、国土安全保障長官は、国家安全保障担当大統領補佐官に、その最初のレビューに基づく委員会の勧告を提供します。

サイバーセキュリティの脆弱性及びインシデントに対応するための連邦政府の方針の標準化

- 大統領令から 120 日以内に、CISA は、他の政府機関及び部門と協力して、連邦一般行政部の情報システムについて、サイバーセキュリティの脆弱性及びインシデントの対応活動を計画及び実施する際に使用される標準的な業務手順を策定します。

連邦政府ネットワークにおけるサイバーセキュリティの脆弱性及びインシデントの検出の向上

- 大統領令から 30 日以内に、CISA 長官は、EDR を実施するための方法に関する勧告を行政管理予算局に提供します。
- これらの勧告を受け取ってから 90 日以内に、行政管理予算局長は、国土安全保障長官と協議の上、連邦一般行政部に属する政府機関が EDR アプローチを採用するための要件を発行します。
- 大統領令から 75 日以内に、各政府機関は CDM プログラムについて、CISA と覚書を作成又は更新します。
- 大統領令から 45 日以内に、国家安全保障局は、国家安全保障システムに影響を与えるサイバーインシデントの検知を向上させるための適切な行動を勧告します。
- 大統領令から 90 日以内に、国防長官、国家情報長官及び国家安全保障システム委員会（Committee on National Security Systems）は、その勧告を検討し、ポリシーを確立します。
- 大統領令から 90 日以内に、CISA は、連邦一般行政部のネットワーク上で、事前の承認なく、脅威探索活動を行うために付与された権限がどのように行使されているかについて報告書を提出します。また、CISA はこの問題について四半期ごとに報告を行います。
- 大統領令から 60 日以内に、国防長官及び国土安全保障長官は、インシデント・レスポンス命令又は緊急指令及び拘束力のある運用指令を共有するための手順を確立します。

連邦政府の調査及び回復（Remediation）能力の向上

- 大統領令から 14 日以内に、国土安全保障長官は、イベントの記録及び関連データの保持に関する要件についての提言を行います。
- これらの提言を受け取ってから 90 日以内に、行政管理予算局長は、商務省及び国土安全保障長官と協議の上、政策を策定します。

国家安全保障システム

- 大統領令から60日以内に、国防長官は、国家情報長官及び国家安全保障システム委員会と連携して、大統領令のその他のサイバーセキュリティ要件と同等又はそれ以上の国家安全保障システム要件を採用しなければなりません。

本稿の原文（英文）につきましては、President Biden Announces Sweeping New Cybersecurity Reforms をご参照ください。

本稿の内容に関する連絡先

奈良房永（日本語版監修）
31 West 52nd Street
New York, NY 10019
+1.212.858.1187
fusae.nara@pillsburylaw.com

嶋村直登 (日本語版作成協力)

Brian E. Finch
1200 Seventeenth Street, NW
Washington, DC 20036
+1.202.663.8062
brian.finch@pillsburylaw.com

Craig J. Saperstein
1200 Seventeenth Street, NW
Washington, DC 20036
+1.202.663.9244
craig.saperstein@pillsburylaw.com

Rose Fowler Lapp
1200 Seventeenth Street, NW
Washington, DC 20036
+1.202.663.8118
rose.lapp@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

田中里美
satomi.tanaka@pillsburylaw.com