protiviti®
Face the Future with Confidence

米国連邦政府機関をはじめさまざまな官民の組織に影響が及ぶと考えられる、国家サイバーセキュリティ強化に関する米国大統領令について

2021
5月14日

5月12日、ジョー・バイデン大統領は「国家のサイバーセキュリティの向上に関する大統領令」を発令しました。この大統領令は、米国の国全体としてのサイバー防衛力を強化して、規模、影響、頻度ともに拡大し続けるサイバーセキュリティの脅威や攻撃に対処するため、政権が打ち出した最新の施策です。これは、連邦政府、公的機関、民間企業のネットワークを保護し、サイバー攻撃が発生した際の国全体の対応能力を強化するとともに、米国政府と民間企業の間の情報共有を改善することを目的としています。

今回の大統領令は、攻撃に対する事後対応から予防へと対策の重点を移行するステップのひとつであり、また、政府と取引するすべての企業にとって、サイバーセキュリティ対策に関し、連邦政府による監督と規制が強化されることを示す新たな兆候です。

この大統領令の対象は、情報技術システム（IT）だけでなく制御系システム（OT）を含み、クラウド、オンプレミス、ハイブリッドクラウドといった環境の別を問いません。米国は世界最大のITサービス購入国であることから、この大統領令で詳述されている目標の実行は、連邦政府機関だけでなく、公共および民間の幅広い組織に影響を与えます。また、より安全なサイバー空間を醸成するため、連邦政府と民間セクターの協力を強化することを呼びかけており、民間セクターが絶えず変化する脅威の環境に適応し、製品・サービスをセキュアに構築・運用して提供することを求めています。

増え続けるサイバー攻撃による米国企業やインフラへの影響

今回の大統領令は、米国における一連の悪質なサイバー攻撃を受けてのものです。2020年には、SolarWinds社のリモートIT管理ソフトウェア「Orion」がハッキングされ、18,000以上の民間および政府機関の顧客のコンピュータシステムが侵害を受けました。今年2月には、フロリダ州の主要な水処理システムが侵入され、水酸化ナトリウムの濃度が人間の消費量よりも家庭用洗剤に適したレベルまで上昇しました。さらに最近では、5月7日にコロニアル・パイプラインがランサムウェアの攻撃を受け、一時的に操業停止とITシステムの凍結を余儀なくされた結果、米国トップの燃料パイプラインが停止し、消費者がガソリンをパニック買いする事態となり、米国の国家および経済の安全保障の脆弱性が露呈しました。これらをはじめとしたサイバー攻撃事案や、国の重要なインフラが攻撃により損害を被る将来のリスクが、米国政府に納入されるソフトウェアのサイバーセキュリティについて、より厳格で拡充された基準を導入することを大統領に決定させる強い動機となりました。

大統領令の主な条項

今回の大統領令は、米国のサイバーセキュリティを強化するためのいくつかの重要な活動に焦点を当てていますが、そのうちのいくつかを以下に要約します。大統領令の全文はこちらをご覧ください。

官民セクター間での脅威情報の共有における障害を取り除くこと。

- 大統領令では、ITサービスプロバイダーが政府と情報を共有できるようにするとともに、具体的な侵害に関する情報を共有することを義務付けています。

プロティビティの視点：この大統領令は米国連邦政府が何を行うかを主に記していますが、問題を解決するために民間組織に求められる実施項目もあります。ソフトウェアのセキュリティを確保すること、サイバー攻撃を報告し対応を支援すること、サイバーセキュリティ安全審査委員会（下記参照）への参加などです。（大統領令は民間からの調達・利

用者としての立場、および民間セクターに対する規制者の立場の両方における連邦政府について記していますが、）規制者としての連邦政府は、民間組織がこれら実施項目に関する基準を満たしているかどうかを確認します。官民の組織には、連邦政府がこれらのサイバーセキュリティ基準をより厳格に課すようになると考えられ、これらの基準を遵守していないと判断された組織が連邦政府と取引する資格を得られなくなる可能性があります。

ソフトウェアサプライチェーンセキュリティの強化により、連邦政府が使用するソフトウェアの安全性と完全性を向上させること。

- 大統領令はソフトウェアのセキュリティを向上するため、連邦政府に納入されるソフトウェアの開発において、ソフトウェア内部に関し透明性を維持することや、セキュリティに関するデータを開示することなど、ベースラインとなるセキュリティ基準を設けます。

プロティビティの視点：今後12ヶ月の間に、商務長官はNISTの長官と協力して、ソフトウェア・セキュリティのための新しい基準とガイドラインを策定し、公開する予定です。これらが策定されると、連邦政府はハードウェアおよびソフトウェア企業にその遵守を強制することになります。さらに、大統領令は、今やはるかに広範な業種や職種に浸透しているデバイスの自動化の進展を特に取り上げています。新たなコネクテッドデバイス（IoTなど）、高速通信（5G）、生産現場への自動化の推進により、データ処理系システムだけでなく、安全性を確保する重要な装置を動かす運用技術、人々が日常的に身につけているデバイスなどについてもセキュリティを考慮することが不可欠となりました。これらの基本的なセキュリティ基準に関連する報告義務がでてくると予想できるため、各組織は、現行のセキュリティ手順を文書化して、今後実施される可能性のある確認対応に備える必要があります。

大規模攻撃への対応を支援し、教訓について学ぶための「サイバーセキュリティ安全審査委員会」を設置すること。

- この大統領令では、重大なサイバーインシデントが発生した際に、政府と民間企業が共同議長を務める「サイバーセキュリティ安全性検討委員会」を設置し、何が起こったのかを分析し、サイバーセキュリティを向上させるための具体的な提言を行うことになっています。

- 理事会は、脅威の活動、脆弱性、リスク軽減活動、政府機関の対応をレビューし、評価を行います。

プロティビティの視点：米国政府の商用ソフトウェアへの高い依存度を考えると、安全審査委員会は、より安全なソフトウェアのための具体的な基準を提供する標準の策定を支援すべきです。また、この新しい安全審査委員会により行われる調査は、国家運輸安全委員会が行う事故調査に類似した厳格なものになるでしょう。各組織は、この規定をどうやって遵守するかについて、将来的に追加のガイダンスを期待するでしょう。

サイバーセキュリティの脆弱性やインシデントに対応するための連邦政府のプレイブックを標準化すること。

- 大統領令は、FCEB（連邦行政部）の情報システムに関するサイバーセキュリティおよび脆弱性対応活動を計画・実施する際に使用する、標準化された一連の運用手順（プレイブック）を作成することとしています。プレイブックには、関連するすべてのNIST標準が参照され、組み入れられます。

- この標準化された手順により、インシデントの情報集約と対処状況の追跡がより協調的かつ集中的に行われ、より効果的で適切な対応が可能になります。

- 政府機関や民間企業がプレイブックから逸脱した手順を採用する場合は、その手順がプレイブックで提案されている基準を満たしているか、それ以上のものであることを証明しなければなりません。

プロティビティの視点：組織は、サイバーセキュリティの脆弱性やインシデントへの対応には、標準化された（または承認された）プレイブックを使用すべきです。これは、効果的な対応を行うために大変重要です。標準的なサイバーセキュリティのプレイブックは、業界や企業の規模によって大きく異なります。多くの組織、特に規制業種以外の組織は、現在のプレイブックを強化するか、新しい基準に沿ったプレイブックの開発に移行する必要が出てくるでしょう。

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上の脆弱性やインシデントの検知を改善すること。

- この大統領令は、政府全体にわたるエンドポイント検知・対応システムの導入と、連邦政府内の情報共有の改善を行うこととしており、それにより連邦ネットワーク上の悪意あるサイバー活動を検知する能力を向上させます。

プロティビティの視点：今回の大統領令に謳われている行動、提言、責務は、連邦政府のネットワークにおける侵入検知の能力を劇的に向上させるはずです。民間企業で存在するものよりもはるかに大きな、世界最大のエンドポイント検知システムを構築するという方向性・指針が示されています。

連邦政府のインシデント調査・修復能力を向上させること。

- 大統領令は、調査担当者がサイバー攻撃の発生源を追跡できるようにするため、連邦政府の各省庁に対してサイバーセキュリティイベントログの要件を設けることとしています。

プロティビティの視点：サイバー攻撃の影響が増大していることを考えると、今こそフォレンジックとイベント調査の能力を向上させることで、将来の攻撃に備えを改善してより迅速な修復ができるようにすべき時です。米国のインフラは、将来のサイバー攻撃に備えるために、このような行動を必要としています。今回の大統領令では、多要素認証（MFA）、データ保管時および転送時の暗号化を義務付けるなど、効果的なサイバーハイジーン（サイバーセキュリティ上の公衆衛生）を可能な限り推し進めようとしていることは明らかです。さらに、企業による、ゼロトラストアーキテクチャ、クラウドコンピューティング、クラウドセキュリティなどの最新のサイバーセキュリティ機能の利用が増えることが予想されます。

今後の展望

この大統領令に対する私たちの今回の解釈では、米国連邦政府と取引を行う企業は、Federal Acquisition Regulation（FAR）や Defense Federal Acquisition Regulation Supplement（DFARS）などの新しい規制が導入されることを想定すべきと考えられます。また、サイバーセキュリティのコンプライアンスを確保するための新たな取締りや、将来のインシデントに対応するための連邦政府機関間の連携とスピードを強化するための新たな仕組みも想定されます。連邦政府機関向けの現行のセキュリティフレームワークは、大統領令による新しいサイバーセキュリティ基準に準拠するように改訂する必要があり、波及的な影響を受けるでしょう。さらに、これらの基準は、連邦政府と協力している組織や連邦政府から助成金を受けている組織にも波及していきます。

プロティビティの支援

プロティビティは、日々進化するサイバー脅威に対応するための準備を支援します。当社の専門家は以下のことができます。

- FAR、DFARS、NIST SP 800-53、NIST SP 800-171、Cybersecurity Maturity Model Certification（CMMC）など米国政府のデータおよびプライバシー保護規制へのコンプライアンスにおける準備、評価、修正の支援
- セキュアでモダナイズされた効率的なクラウドコンピューティング環境への移行における適切な評価、計画、実行の支援
- サイバーセキュリティのインシデント対応計画、実行、緊急対応、危機管理の支援
- ゼロトラスト原則や NIST 800-207 などを基にした、環境全体（クラウドやオンプレミスなど）におけるゼロトラストアーキテクチャへの移行に関する評価、計画、実行の支援
- デジタル資産の保護を強化するための多要素認証および暗号化ソリューションの評価、計画、導入、自動化

詳細については、プロティビティ（tokyo@protiviti.jp）にお問い合わせください。

protiviti®