

リスク管理を含むSW運用・開発統合基盤を支える思想とその経緯ーDoWのオープンアーキテクチャの取組ー(前編)

株式会社 Japan Aerospace & Defense Consulting
株式会社 SHIFT

菅野 隆 澤田 栄浩

本シリーズでは、DoWにおけるサイバーセキュリティのリスク管理についての理解を深めることを目的とし、主に2000年以降の「情報保証」から、サイバーセキュリティCS (Cyber Security) のリスク管理枠組みRMF (Risk Management Framework)、そして、その進化形として国防総省 (DoD) が昨年、推進開始を宣言したCSRMC (Cyber Security Risk Management Construct) に至る経緯などについて触れてきました。

本稿では、CSRMCが組み込まれたSW (ソフトウェア) 定義型防衛システムを支えるオープンスタンダードアーキテクチャ (Open-Standard Architecture) の考え方、枠組み・コンソーシアムなどについてレビューした上で、シリーズを総括します。

前編では、ソフトウェア定義型防衛システムを支える主要な考え方を中心に述べていきます。

はじめに

冷戦後、米国連邦政府による公開以降、インターネットは瞬く間に世界に拡大・普及しました。ユーザーが激増するとともに、新しい技術と思想が生まれて発展しました。防衛技術に焦点を当てると、防衛分野の技術開発が先端技術を牽引する、それまでの「スピノフ (Spin-Off)」の流れから、民間で洗練された当時の最も効果的なベストプラクティスが防衛分野へと取り込まれるという、新しい流れが形成されているように見えます。

この取り組みは、冷戦後の情勢下、DoDにおいて1994年のペリー・メモを起点として、コストのかかる防衛規格 MIL-SPEC (Military Specification の略) から標準化に向けた取り組みが開始され¹⁾、2010年代に、デジタル技術を活用する効率化、Digital Engineering 推進に

舵を切ることで促進されています。その中で「兵器システムのSWによる能力向上」の傾向が次第に顕著になっていきます。

本シリーズで取り扱ってきた「リスクが存在するものとして、それを管理する」といった思想をベースとしたRMFは、CS黎明期の2010年代、そこでの安全を確実なものとするためのコンプライアンス手続きとして開始されました。自動化技術を活用して、ライフサイクルを通じた全プロセスの継続的な監視、そして、リスクが検知された場合は速やかに対応 (改善) し、その後、切れ目なく承認するといったレジリエンス重視の方向に進んできたのは、ごく自然な流れです。これらに活用される機能とそのメリットは、兵器システムの能力向上が「PF (Platform) 中心からSW (Software) 中心」に移行する中、兵器システムのSWの開発、運用、能力向上のプロセスに求める機能と共通しており、あるいは親和性が高いものです。

本シリーズでは、戦争省（DoW）が2025年以降に構築を目指している CSRM C は、主にソフトウェア定義型防衛システム（Software-Defined Defense System）を、AIを活用して効率的・安全に開発、運用するためのリスク管理を含んだ、自動化された統合基盤を目指している状況であることも紹介してきました。

本稿では、CSRM C が組み込まれた SW 定義型防衛システムを支えるオープンスタンダードアーキテクチャ（Open-Standard Architecture）の技術要素、枠組み・コンソーシアムなどについてレビューした上で、シリーズを総括します。

ソフトウェア定義型防衛システムを支える仕組み

(1) 共通

ア DE（Digital Engineering）

「複雑化したシステムをモデルで管理する」

DE は「デジタルモデルおよびそれを支える基盤データを、DoD におけるシステム情報の開発、伝達、および管理の主要な手段として活用すること」と定義され、デジタルモデルペー

スのデータ中心の包括的アプローチです。このアプローチは、Digital Engineering Ecosystem、Digital Model、Digital Thread、Digital Artifacts で構成され、その代表的な成果物の一つとして Digital Twin が挙げられます²⁾（表 1、図 1）。

DE の基礎となったのが Modeling & Simulations（M&S）です。DoD における M & S は、現実の兵器システム等のモデルを作成し、様々な前提や条件下、コンピュータ上で単独で、あるいは組み合わせて動作させ、その挙動を予測するアプローチです。そして、それを実現するためにはデータが必要不可欠です。

データの標準化に関し、1994年12月、DoD の監察総監室 OIG（Office of the Inspector General）は、デジタル MC & G（Mapping, Charting, and Geodesy）データの標準化推進状況^{*1}と（軍民）相互運用性評価について報告しています³⁾。前出のペリー・メモは同年6月29日の日付であることから、同報告書は標準化・共通化に向けた取組の一つと考えられます。

表 1 Digital Engineering Framework

Digital Engineering Ecosystem	Digital Model	Digital Thread	Digital Artifacts
DE 実現のための基盤環境 【構成要素】 ・ハードウェア ・ソフトウェア ・ネットワーク（クラウドを含む） ・ツール ・人材 【アプローチ】 ・プロセス 開発、テスト、製造等 ・方法論 MBSE 等 ・実践手法 DevSecOps 等 【イメージ】 ・MBSE（Model Base Systems Engineering）ツール ・PLM（Product Lifecycle Management）システム ・シミュレーション環境 ・データ管理環境 ・DevSecOps 基盤 ・標準化されたプロセスが統合された環境全体	システム情報の主要な表現手段 ・要求モデル（Requirements Models） ・構造モデル（Structural Models） ・機能モデル（Functional Models） ・アーキテクチャモデル（Architecture Models） ・エンタープライズモデル（Enterprise Models） ・物理モデル（Physics-Based Models） ・人的性能モデル（Human Performance Models） ・ライフサイクルモデル（Product Lifecycle Models） ・デジタルツイン（Digital Twin）	デジタルモデル同士やデータをつなぐ仕組み（ライフサイクルを結ぶ情報連携） 一例 要求→アーキテクチャ→設計→製造→試験→運用→維持整備 という情報連鎖	デジタルモデルから生成される成果物 ・設計仕様書 ・技術図面 ・設計文書 ・Interface Management Document ・解析結果 ・BOM（部品表） ・ソースコード ・WBS ・製造指示書 ・テストケース ・スケジュール

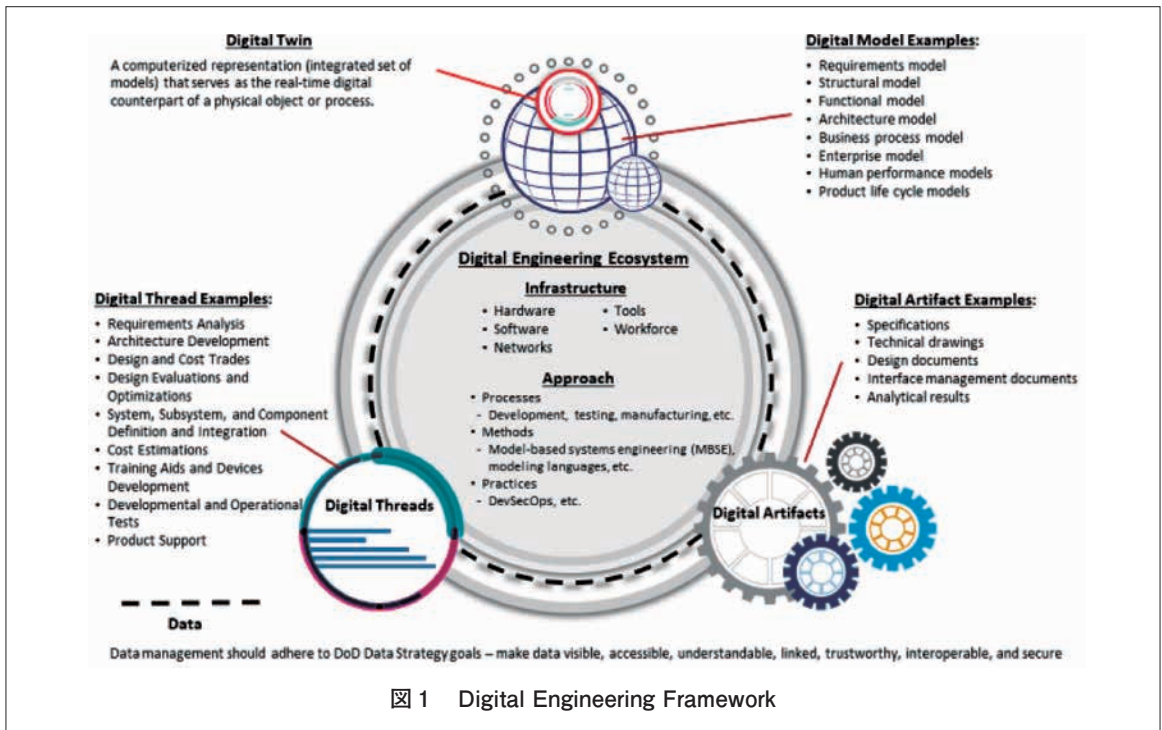


図1 Digital Engineering Framework

1994年、DoD Directive 5000.59 “M&S”を発令、データ管理の基礎を築きます。そして2007年に同指令を改訂し、M&Sを「DoDの活動を支える重要な実現基盤」と位置付けるとともに、その体制を整え、（各機関、軍種間の）相互運用性と構成要素の再利用を促進するための方針を提示しました。その鍵となるのが、運用を通じて蓄積される膨大なデータに他ならず、この指令はデータ戦略の基準を築いたと評価されています⁴⁾、²⁾。

これらの取組等の積み上げを基礎として、2018年、DE戦略が正式に発表され、DEの定義が確立³⁾されるとともに、五つの戦略目標⁴⁾が提示されています⁵⁾、⁵⁾。

更に2019年にはDoD デジタル近代化戦略（2019～2023）が公開されました。これは2014年策定の「DoD 情報資源管理戦略」を全面的に置き換える包括的な戦略の位置付けであり、DEを「防衛調達において、新しいテクノロジーを省内に迅速に取り込むための「革新的な技術開発手法（innovative technology development

practices）の代表例」「国防総省全体におけるソフトウェア配信のコストや統合速度を効果的に管理・効率化するアプローチ」と具体的・明確に位置づけました⁶⁾。

2023年に発令された DoDI5000.97では、防衛取得プログラムのライフサイクル全体において、DEの方法論・技術・実践を使用することを基本とすることを方針化するに至っています⁷⁾。

イ OSS（Open Source Software）

「戦場の優位性の確保するためのスピードとゼロトラストの両立」

DoDは、OSSを「人間が読めるソースコードが、そのソフトウェア利用者による使用、研究、再利用、修正、機能強化および再配布のために利用可能なソフトウェア」と定義しています。

ARPANET 研究開発に関わった当時のコミュニティにおいては、ソースコードや研究成果を共有することは慣行でした。そしてそれは、コードにバグが発見されてもすぐにパッチ処置が施され、わずかな時間で改善されると

いった個々の研究者の創造的な力をコミュニティ全体で享受できる文化でした^{*6}。1990年代、インターネットが公開されて商用SW会社が急成長すると、SWは購入するものという考え方が主流となりましたが、2000年頃以降OSSも同時に急成長しました。しかしながら、当時のDoDにおいては、OSSの使用が奨励されていた訳ではなく、OSSにはセキュリティ上のリスクがあるという雰囲気が存在していたと言われています。

2003年になって、DoD CIOの覚書“OSS in the DoD”において、ようやくOSS利用を明示的に「容認」する統一見解が示され、それ以降、Linuxサーバー、OpenBSD、GCCコンパイラなどがDoD内部でも導入されるようになります（このSW近代化とセキュリティ管理を両立した活用指針が同政策の出発点と言われています⁸⁾⁻¹⁰⁾。2009年には、旧覚書を置き換える形で、OSS利用を巡る考え方をより明確化・具体化し、「積極的な活用」を促す指針としての覚書が発出されました¹¹⁾。そして2017年に、OSSコミュニティの支援を受け、DoDのOSSサポートに関するガイドラインを策定し、DoDのOSSコード公開、OSSコミュニティとの連携促進と省内向けガイダンスを目的としたコードミル (<https://code.mil/>) が開設されています。2018年に発効したDoDサイバー戦略においては、OSSをデジタル変革、クラウド活用、DevSecOps、AI開発の基礎として位置付け、2022年の覚書においては、DoDにおけるOSS活用を「推奨」することが明文化されるに至ります¹²⁾。OSSのリスク管理の考え方は、RMFやZero Trust(後出)と共通のものといえます。

DoWは、サイバーセキュリティ上のリスクを経てもなお、OSS活用のメリットがより大きいとの判断の下、OSSをソフトウェア近代化戦略の中心要素の一つに位置づけています。

ウ Zero Trust

「システムの内側も信用しない」

Zero Trust (ZT) のアイディアの萌芽は

1990年代に遡りますが、2000年頃以降に注目され始め、2010年代に入って概念が具体的に提唱されて広く知られるようになりました。「決して信頼せず、常に検証する」という基本理念をベースとしたITセキュリティモデルのことで、従来からあった境界型セキュリティの考え方とは対極的な発想であり、ネットワークの内側を含め、都度厳格な認証・認可を求める考え方です。

この基盤的な考え方導入の転機となったのが、2019年に始まった新型コロナウイルス(COVID-19)の世界的パンデミックに伴うDoD内でのリモートワークへの急速な移行でした。クラウドベースの技術やAI活用への移行が進むと同時に、同盟国や防衛産業基盤DIB(Defense Industrial Base)などのパートナーとのネットワークを通じた連携機会が増加しました。結果として保護すべき対象領域、機密データを流出させる手段・機会が拡大したため、場所や境界に依存しないアプローチが求められるようになり、2020年に国立標準技術研究所から、NIST SP800-207(ZT)が公表され、その定義が確立することになります。

そして連邦政府の取組を最も強く促したイベントが同時期の2019年、ロシア対外情報庁によるものとされるSolarWinds攻撃(SolarWinds Hack)と言われています。2019年9月頃に開始されたとみられるSolarWinds社への侵入が、2020年11月頃まで検知されず、その間に脅威アクターによりトロイの木馬化されたコードが注入されたアップデートデータによって政府機関の情報システムが感染、このコンピュータが脅威アクターに「バックドア」を提供していた状況に一定期間気付かなかったというのが事の顛末です¹³⁾。また2021年のコロニアル・パイプライン社は、使用していないVPNアカウントを悪用された侵入によりランサムウェア攻撃を受け、身代金の支払いを行ったと言われています¹⁴⁾。更に2021年に発見されたLog4Shell脆弱性^{*7}は、発見された時点で「全てのクラウド

環境の93%が危険にさらされていた」と言われているゼロデイ脆弱性でした。そして、Github^{*8}に脆弱性を改善する目的のPoC(Proof of Concept:概念検証)コードが投稿されると、ハッカーによる攻撃が開始され、他国の国家機関までもがこれに加わったと言われています¹⁵⁾。

これらのサイバー攻撃を受け、2021年5月に「国家サイバーセキュリティ向上に関する大統領令(EO14028)」¹⁶⁾が発令されました。そこで、「漸進的な改善では必要なセキュリティは確保できず、大幅な変更と多大な投資が必要」との危機感を示した上でZTアーキテクチャへの移行の方針を明示し、2022年、CS関連に過去最高規模の予算が配分されました。その中にはZT、CMMC(後出)の導入のための予算が含まれていました。そして、これらの投資を効果的なものとするために、連邦ZT移行戦略(2022.1.26)¹⁷⁾、国家安全保障覚書第8号(2022.1)¹⁸⁾、^{*9}などの一連の命令が発効、ZTへの移行を義務付けます。これを受け国防省も、ZT戦略およびそのロードマップを策定、2027年度までに目標レベルに達成すべく取組に着手しています。

令和6年版防衛白書によると、防衛省は「境界型セキュリティのみで組織ネットワーク内部を安全に保ち得るという従来の発想から脱却し、ZTの概念に基づくセキュリティ機能の導入に向けた取り組みを進めていく。これらにより防衛省・自衛隊のCSを向上させ、万が一、組織ネットワーク内部に侵入されたとしても迅速に検知、対処できる態勢を構築する」とし、2027年の運用開始を目指している模様です¹⁹⁾。

(2) ネットワーク

Cloud

「ミッション即応性に対応するためのセキュリティと相互運用性を提供」

Cloud Computingの概念は1960年代に既に提唱されています²⁰⁾。その後、インターネットの普及に伴いのそのワードが頻繁に使用される

ようになり、2006年、AWSがサービスの提供を開始します。

DoDは長年にわたり、軍種・組織ごとに個別にITシステムを構築してきましたが、その結果、データ分散、組織間の連携困難、重複投資、セキュリティ管理の複雑化といったIT特有のストープパイプ^{*10}の課題を抱えるようになっていました。

2014年に発出されたDoD CIOの覚書は、商用クラウドサービスの取得ガイダンスを更新するもので、DoD組織の商用クラウドサービスの直接調達を可能にしました^{*11, 21)}。またFedRAMP^{*12}のよるベースライン、認証、CAP(Cloud Access Point)集約化などDoD内でのルールを共通化することによるクラウド活用に向け踏み出した一歩に位置づけられます。

そして2017年、DoDは共通クラウド基盤であるJoint Enterprise Defense Infrastructure(JEDI)を導入する方針を打ち出します。DoD全体としての従来の課題の解消を目指すとともに、AI基盤整備、C2システムの統合などを企図した野心的な巨大プロジェクトでした。2019年にMicrosoft社が受注したものの、単一ベンダー方式などであったため、訴訟を含む激しい論争となり、2021年7月に中止に至ります。DoDは、この機能を実現するため、マルチベンダー、マルチクラウド方式のJoint Warfighting Cloud Capability(JWCC)を改めて打ち出し、Microsoft社、Amazon Web Service社、Google社、Oracle社などと契約を締結しました。JADC2、AI、データ共有基盤などの移行は継続中の模様です²²⁾。

最近のトピックとして、フランス政府は、国の技術・法的保護と技術自立を重視しソブリンクラウド^{*13}を中心の概念とし、信頼できるクラウド認証、クラウド中心行政、産業競争力強化を柱とした国家クラウド戦略を公表しています。現在の厳しい安全保障・経済安全保障の環境下、データやSWの主権を保持管理する視

点は、独立国家として極めて重要であるといえます²³⁾。わが国の防衛省は、令和9年度概算要求パンフレットにおいて「(防衛省クラウドの整備にあたり、) 高安全性と主権性を確保した機密ソプリングクラウドの導入を進める」としています。

(3) ソフトウェア開発環境

DevSecOps (Development・Security・Operations)

「継続的にソフトウェアを更新する」

DevSecOpsとは、ソフトウェアの開発(Development)、セキュリティ(Security)および運用(Operations)を統合することを目的とした、組織的なSWエンジニアリングの文化および実践のことを指し、迅速で安全なSW開発における業界のベストプラクティス・運用思想とされます²⁴⁾。

三つのプロセスを統合することで、自動化や継続監視を通じ、高品質な成果物を生む手法

で、SWライフサイクルの全フェーズ(計画、開発、ビルド、テスト、リリース、配信、デプロイ、運用、監視)におけるセキュリティの確保を目指しています。また自動化された単体テスト、機能テスト、統合テストおよびセキュリティテストにより、テストとセキュリティが「シフトレフト(フェーズの初期段階に前倒し)」されるといった効果があります。

DevSecOpsを実現する人、インフラストラクチャ、デジタルプラットフォーム、アプリケーションのツール、そのプロセスの集合体は、「SWファクトリー(Software Factory)」と呼ばれ、実現するための必要なツール・サービスのベストプラクティスの選択肢は、既に民間において多数存在しています。DoDにおいては、SWファクトリーとして、Platform One^{*14}、Black Pearl^{*15}、Kessel Run^{*16}、Army Software Factory^{*17}などが既に稼働しています。

(つづく)

注

- * 1 防衛や民間システム全体で地理情報、地形、水路データを共有・活用するための統一規格のこと。
- * 2 DoDのデータ戦略については、別途テーマとして今後取り上げる予定。
- * 3 デジタルエンジニアリング(定義): コンセプト(構想)から廃棄に至るまでのライフサイクル活動をサポートするために、分野横断的な連続体(Continuum)として、システムデータとモデルの信頼できる情報源(Authoritative Sources)を使用する、統合されたデジタルアプローチ。
- * 4 ①エンタープライズおよびプログラムの意思決定を支援するための、モデルの開発・統合・使用の形式化②永続的で信頼できる「唯一の情報源(Authoritative Source of Truth)」の提供③エンジニアリング実務を向上させるための技術革新の導入④関係者間での活動、協働、コミュニケーションを支援するインフラと環境の構築⑤ライフサイクル全体を通じてデジタルエンジニアリングを採用・支援するための文化と人材の変革。
- * 5 このタイミングに合わせて出版されたDoDD5000.59は時点修整(組織再編に伴う更新)の位置付け。
- * 6 多くの大学や研究機関が軍事研究プロジェクトを通じ、ソフトウェアを共同開発していた。UnixやTCP/IPなどの重要技術も政府研究資金により発展し、改良を共有していた。
- * 7 Log4Jとは広く普及したOSSのライブラリであり、そこで提供されたLog4Shellに存在した脆弱性。悪意のある攻撃者はこのLog4Jの脆弱性を利用して、脆弱なシステム上でほぼ任意のコードを実行することが可能であった。
- * 8 ソースコードをオンライン上で共同開発できるOSSのソフトウェア開発PF。
- * 9 国家安全保障システム(NSS)に適用するための文書。
- * 10 組織の複数部門が調整なく個別にシステムを構築することで、結果的にコストがかかり、データ、セキュリティなどに相互運用性が欠如する傾向が強いといった縦割り(セクショナリズム)を表すIT用語。
- * 11 この覚書以前、商用クラウドサービスを取得するためには、DISA(Defense Information Systems Agency)経由に限定されていた。
- * 12 Federal Risk and Authorization Management Program。2011年開始の連邦政府が利用するクラウドセキュリティ認証制度。NISTなどが中心となり策定し、連邦政府全体のクラウド認証プログラムとして運用中。なおDoDの場合、加えてDoD Security Requirements Guide(SRG)による認証が必要。Azure Government、AWS Gov Cloudは両社の要求を満たしている。
- * 13 関係サーバの運用・管理を国内に限定し、外国法規制の影響を受けずに「データ主権」を確保可能なクラウドサービスのこと。現時点では日本国内において明確に定義されていない。
- * 14 米空軍が中心となって構築した、DoD全体向けのエンタープライズDevSecOpsプラットフォーム、共通基盤。DoDがSWを迅速・安全に開発・配備するためのSWファクトリーの代表例。<https://pl.dso.mil/>

- *15 米国海軍が推進する、エンタープライズ DevSecOps プラットフォーム、共通基盤であり、海軍全体の SW 開発を支える SW ファクトリー。 <https://blackpearl.navy.mil/va.us/perry94.html> (Accessed on 23 July, 2026)
- *16 米空軍の SW ファクトリーとしての環境の整った組織。 DoD におけるアジャイル開発と DevSecOps の先駆者と意義づけられている。 2017年に設立され、正式名称は Air Force Life Cycle Management Center (AFLCMC) Detachment 12。
- *17 米陸軍の SW ファクトリーとしての環境の整った組織。 2021年設立。 人材育成とアプリケーション開発を重視。

参考文献

- 1) Memorandum of Specifications and Standards by the Secretary of Defense 29 Jun 1994, <https://sw-eng.falls-church.va.us/perry94.html> (Accessed on 23 July, 2026)
- 2) DoD “Digital engineering Strategy”, Office of the Deputy Assistant Secretary of Defense for System Engineering, June 2018. https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf (Accessed on 27 July, 2026)
- 3) Office Of The Inspector General, “Audit Report: Digital Mapping Charting, and Geodesy Data Standardization. Report No. 95-060”, December 19, 1994. <https://media.defense.gov/1994/Dec/19/2001714847/-1/-1/1/95-060.pdf> (Accessed on 27 July, 2026)
- 4) DoD Directive 5000.59 “DoD Modeling and Simulation (M&S) Management”, August 8, 2007 <https://www.acqnotes.com/Attachments/DoD%205000.59%20Modeling%20and%20Simulation.pdf> (Accessed on 27 July, 2026)
- 5) DoD “Digital engineering Strategy”, June, 2018. https://ac.cto.mil/wp-content/uploads/2019/06/2018-Digital-Engineering-Strategy_Approved_PrintVersion.pdf (Accessed on 27 July, 2026)
- 6) DoD “DoD Digital Modernization Strategy, DoD Information Resource Management Strategic Plan FY19-23”, Department of Defense Office of Prepublication and Security Review, Jul. 12, 2019, <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF> (Accessed on 27 July, 2026)
- 7) DoDI 5000.97 “Digital Engineering” December 21, 2023 (Effective) <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500097p.PDF> (Accessed on 27 July, 2026)
- 8) 菅野, 澤田, “新たな領域が防衛力ドメインに追加された背景 (2)” JADC-HP, <https://shift-jadc.jp/report/20251128/> (Accessed on 15 Aug. 2026)
- 9) Memorandum by CIO, DoD, “Open Source Software (OSS) in the Department of Defense (DoD)”, May 28, 2003, https://terrybollinger.com/stenbitmemo/stenbitmemo_pdf.pdf (Accessed on 15 Aug. 2026)
- 10) Patricia Daukantas, “Open-source software gets nod from DOD”, Route Fifty HP, Jun.23, 2003, <https://www.route-fifty.com/digital-government/2003/06/open-source-software-gets-nod-from-dod/278099/> (Accessed on 15 Aug. 2026)
- 11) Memorandum by CIO, DoD, “Clarifying Guidance Regarding Open Source Software (OSS)”, Oct. 16, 2009, <https://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf> (Accessed on 15 Aug. 2026)
- 12) Memorandum by CIO, DoD, “Software Development and Open Source Software”, Jan. 24, 2022, <https://dodcio.defense.gov/Portals/0/Documents/Library/SoftwareDev-OpenSource.pdf> (Accessed on 15 Aug. 2026)
- 13) GAO Post, “SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)”, April 22, 2021. <https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic> (Accessed on 31 July, 2026)
- 14) Jack Beerman, et al., “A Review of Colonial Pipeline Ransomware Attack”, 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops <https://www.computer.org/csdl/proceedings-article/ccgridw/2023/020800a008/10Un8x1LGus> (Accessed on 31 July, 2026)
- 15) “Log4j の脆弱性とは何ですか” IBM-HP <https://www.ibm.com/jp-ja/think/topics/log4j> (Accessed on 15 Aug. 2026)
- 16) Executive Order 14028 of May 12, 2021, “Improving the Nation's Cybersecurity”, Federal Register, <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity> (Accessed on 31 July, 2026)
- 17) OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf> (Accessed on 30 July, 2026)
- 18) Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, January 19, 2022, <https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/> (Accessed on 31 July, 2026)
- 19) 『令和 6 年版防衛白書』防衛省2024 http://www.clearing.mod.go.jp/hakusho_data/2024/html/n310405000.html (Accessed on 30 July, 2026)
- 20) Giulia Borgoni, “The Evolution of Cloud Computing: From the Early Ideas of John McCarthy to Modern Platforms”, Jun. 24, 2025, Elemento Modular Cloud-HP, <https://elemento.cloud/blog-posts/2024-11-11-the-evolution-of-cloud-computing-from-the-early-ideas-of-john-mccarthy-to-modern-platforms.html> (Accessed on 15 Aug. 2026)
- 21) https://dodcio.defense.gov/portals/0/documents/cloud/dod_cio-updated_guidance-acquisition_and_use_of_commercial_cloud_services_20141215.pdf (Accessed on 30 July, 2026)
- 22) <https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF>
- 23) 「ソブリンクラウド」 NEC-HP, <https://jpn.nec.com/cloud/service/concept/sovereign/index.html> (Accessed on 17 Aug., 2026)
- 24) DoD Enterprise DevSecOps Reference Design, Department of Defense (DoD) Chief Information Officer 2019, https://dodcio.defense.gov/Portals/0/Documents/DoD_Enterprise_DevSecOps_Reference_Design_v1.0_Public_Release.pdf (Accessed on 31 July, 2026)