国防総省におけるサイバーレジリエンスの強化

自動応答と相互運用性によって永続的な優位性を構築

「サイバーレジリエンス：サイバーリソースを使用する、またはサイバーリソースによって実現されるシステムに対する悪条件、ストレス、攻撃、または侵害を予測し、それに耐え、そこから回復し、適応する能力」

米国国立標準技術研究所 (NIST)

「[国防総省] は統合軍のサイバーレジリエンスを強化し、争いが起こる、過密状態のサイバー空間で戦い抜く能力を確保します。統合軍の軍事任務の遂行を支援するサイバー能力を優先し、ネットワークと戦闘プラットフォームの機能が低下しても任務を遂行できるよう部隊を訓練することに尽力します」

2023 年 米国防総省サイバー戦略[1]

大国間の競争にはサイバーレジリエンスが必要

サイバーレジリエンスは、国防総省 (DoD) 全体で継続的な作戦即応性を維持するための基盤です。敵意が渦巻く過密状態のサイバー空間で戦い抜くために、部隊には以下の能力が必要です。

- **機動性：**サイバーオペレーターは、破壊されたアプリケーションや機能が低下したアプリケーションを、パブリッククラウド、駐屯地または基地のデータセンター、あるいは戦術的エッジ (例：航空機、船舶、車両、ポータブル・フライアウェイ・キット) など、同じ場所または別の場所で迅速に復元できなければなりません。
- **相互運用性 (取り組みの一体化と多機能部隊を実現するため)：**各サービスコンポーネントでは、複数のベンダーのサーバーとネットワークデバイスが使用されます。マルチドメイン運用 (MDO) では、サイバーオペレーターは、ソフトウェアの更新、設定の変更、容量の追加、およびレジリエンスに必要なその他のアクションに関するベンダー固有のコマンドを知らなくても、あらゆるベンダーのデバイスを管理できる必要があります。
- **アプリケーションの迅速なデプロイとスケーリング：**国防総省の科学チームと開発者は、攻撃的および防御的なサイバー作戦や意思決定の優位性に使用される人工知能および機械学習 (AI/ML) モデルとアプリケーションの再トレーニングとチューニングを継続的に行っています。新たな脅威に直面した際のレジリエンスには、モデルトレーニングの容量を迅速に拡張できること、また、戦闘員に最も近い場所にあるハードウェアに関する特別なトレーニングを受けていなくても、その場所に新しいモデルをデプロイできることが必要です。
- **サイバー領域全体の可視性：**オペレーターは、新たな脅威の発生源を特定して効果的な対策を講じることができるように、サイバー領域を確実に可視化する必要があります。

Red Hat テクノロジーがサイバーレジリエンスを加速

国防総省は、自動化と相互運用性を実現する Red Hat® テクノロジーを使用して、サイバーレジリエンスを加速できます。Red Hat Ansible® Automation Platform は、破壊されたり能力が低下したりした機能の回復を自動化し、迅速な任務の遂行を支援します。Ansible Automation Platform は自然言語で表現された意図 (例：「新しいルートを追加する」) を各デバイスに適切なコマンドに変換するため、サイバーオペレーターはサービスの設定、デプロイ、拡張のためにベンダー固有のコマンドを習得する必要がありません。

Kubernetes をベースとするハイブリッドクラウド・アプリケーション・プラットフォームの Red Hat OpenShift® は、コンテナ化されたアプリケーションと仮想マシン (VM) を、ほとんどまたはまったく変更を加えることなく、任意の場所にあるさまざまなベンダーのサーバーハードウェアに移行できるようにすることで、レジリエンスを加速します。たとえば、基地のデータセンターが破壊された場合でも、そのアプリケーションをパブリッククラウドに復元できます。その逆も同様です。ワークロードは、Red Hat Device Edge を実行する戦術的エッジ (航空機、車両、船舶、ポータブル・フライアウェイ・キットなど) のリソースに制約のある小型デバイスでも実行できます。Red Hat Device Edge を実行しているエッジデバイスは、ネットワーク接続が拒否される、中断する、断続的になる、制限される (DDIL) 状況でも動作し、接続が利用できない場合でもデータの収集と分析を継続します。

1 「2023 Cyber Strategy of the Department of Defense」(media.defense.gov)、2025 年 1 月 13 日にアクセス。

「セキュアでレジリエントな C3 [指揮 (Command)、統制 (Control)、通信 (Communications)] 機能は、戦場での確実で信頼できる情報交換に不可欠です」

国防総省[2]

サイバーレジリエンスのシナリオ

機動性の自動化

任務の課題：プライマリーサイトが攻撃を受けている場合、セカンダリーサイトまたは三次サイトへの従来のフェイルオーバーには 1 時間以上かかる可能性があり、任務の存続が脅かされます。

Red Hat によるサポート：Ansible Automation Platform は、任務を危険にさらすイベントを検出すると、事前に定義されているアクションの Playbook を自動的に実行し、ほぼリアルタイムでリスクに対処します。プライマリーサイトが動作不能になった場合、Ansible Automation Platform と Red Hat OpenShift が連携して、ミッションクリティカルなワークロードをセカンダリーサイトまたはリカバリーポイント (基地、パブリッククラウド、エッジサーバーなど) に自動的に移行します。人間の介入は不要です。代わりに、Event-Driven Ansible と呼ばれる機能が通信回線やサーバーの障害などの状況を監視し、自動化されたアクションを実行して、代替の場所からサービスを再構築します (表 1)。Red Hat OpenShift は、アプリケーションがどこで実行されているかに関係なく一貫して動作できるようにします。成熟し、自動化されたワークフローは、運用継続性 (COOP) の目標をサポートします。

表 1. Ansible Automation Platform が認識および修復できる有害なイベントの例

脅威	脅威に対抗するための Playbook アクションの例
通信回線に障害が発生	ワークロードを代替サイトに移行する
マルウェアの検出	感染したシステムをオフラインにして、リアルタイムで新しいシステムを立ち上げる アプリケーションサービスをスケールアップまたはスケールダウンする ファイアウォールのポートを閉じる
クラスタノードが応答を停止	別のノードでワークロードを再構成する
VM またはコンテナ上の構成ドリフトによってセキュリティ脆弱性が発生	自己修復アクションを特定して実行する

サイバー領域全体での取り組みの一体化

任務の課題：各サービスコンポーネントでは、多くの OEM (相手先ブランド名製造) のサーバーとネットワークデバイスが使用されており、それぞれが独自の管理ツール、オペレーティングシステム、コマンドを備えています。1 つの部門内でも、サイバーオペレーターはデプロイを管理するためにさまざまなツールセットに関するトレーニングを受ける必要があります。

Red Hat によるサポート：Red Hat OpenShift を使用すると、アプリケーションを一度構築すれば、ハイブリッドクラウドからエッジまでどこにでもデプロイできます。つまり、1 つの部門またはコンポーネントによって開発された ML モデルや AI ベースのアプリケーションを他の部門またはコンポーネントのサーバーにデプロイできるため、取り組みの一体化と多様な能力を備えた IT 人材の育成が促進されます。また、自動化は取り組みの一体化に役立ちます。各部門の IT スペシャリストは共通の作戦能力の実現を目

2 「DoD Releases the Fulcrum: DoD Information Technology (IT) Advancement Strategy」(defense.gov)、2024 年 6 月 25 日。

指して作業できるようになり、多数の IT システムそれぞれに固有のテクノロジーコマンドを習得する必要もないからです。Ansible Automation Platform は、コマンドライン・インタフェース (CLI) またはアプリケーション・プログラミング・インタフェース (API) から開始できるあらゆるアクションを自動化できます。

「…国防総省は、関連する任務の要素の可視性、機能、運用を統合することにより、防衛サイバースペースと DODIN [国防総省情報ネットワーク] 運用を結ぶ取り組みの一体化を高めます。DODIN が進化するサイバー脅威に迅速に対応できるようにするため、インテリジェンス、取得と維持、その他の機能を連携させます」

2023 年 米国防総省サイバー戦略[2]

戦闘能力の大規模かつ迅速な構築とデプロイ

任務の課題：国防総省のソフトウェアチームは、ストレスや攻撃に応じて継続的にソフトウェア機能を追加し、セキュリティを強化し、ML モデルをチューニングしています。現在、各ドメインで複数のハードウェア・プラットフォームが使用されており、その一部は DDIL 環境で動作しているため、ソフトウェアの更新サイクルに遅れが生じています。サイバーレジリエンスを加速するには、サービスコンポーネントが新しいアプリケーションや更新されたアプリケーションをさまざまなエンドポイントに迅速かつ大規模にデプロイでき、アプリケーションがすべてのプラットフォームで一貫して動作するようにする必要があります。

Red Hat によるサポート：Red Hat OpenShift を使用することで、共同作戦チームが一度構築したアプリケーションは、データセンター、クラウド、軍務用エッジなど、あらゆる環境にデプロイできるようになります。VM は同じノード上のコンテナと並行して実行できるため、運用が単純化され、リソースの使用が最大化されます。脅威や悪条件に直面した場合、部隊は必要に応じて容量を自動的に拡張できます。

共同作戦チームは、Red Hat OpenShift、Ansible Automation Platform、Red Hat Device Edge を組み合わせて使用することで、地理的に制約のあるエリアに標準化された AI 機能をデプロイできます。たとえば、ある前方作戦基地 (FOB) で、ドローン画像を撮影してその特徴を解析する ML モデルの更新が必要だとします。Red Hat Device Edge を使用すると、Stalker 無人航空システム (UAS) のような米国の軍用プラットフォームに高度なソフトウェアを搭載して、小規模なプラットフォームで大規模な AI ワークロードを処理できるようになり、戦場でより迅速なデータに基づく意思決定を促進できます。このシナリオでは、Ansible Automation Platform によってオペレーターは Playbook を実行し、更新されたモデルを多数のドローンやその他のエッジデバイスに同時にデプロイすることができます。その結果、エラーを削減し、運用の一貫性を向上し、実際の脅威情報と任務のニーズにより迅速に対応できるようになり、任務の成果が加速されます。

サイバー領域全体の可視性と可観測性

任務の課題：国防総省は、コンプライアンスプロセスの効率化やリスクの軽減のほか、セキュリティ技術実装ガイド (STIG) の導入、パッチ管理、設定管理、インシデント対応などの重要なタスクの自動化に取り組んでいます。成功の障壁としては、大規模攻撃によるサイバー暴露リスク、安全保障環境と国防総省の軍事力態勢の継続的な変化、急速に変化する技術などがあります。

Red Hat によるサポート：Ansible Automation Platform は、IT 資産の包括的なインベントリーを提供し、サイバー領域 (ハイブリッドクラウド、オンプレミス、エッジ) 全体の可視化を可能にします。正確で最新のインベントリーにより、国防総省の IT チームは、より迅速に拡張し、コンプライアンス リスクを軽減し、可用性に対する脅威をすばやく特定して修復することで、レジリエンスを加速できます。

サイバー領域全体でリアルタイムイベントを観察するには、Ansible Automation Platform に付属している Event-Driven Ansible を使用します。Event-Driven Ansible は指定されたイベントを継続的に探し、イベントが検出されると事前に定義されているアクションを自動的に呼び出します。

3 「2023 Cyber Strategy of the Department of Defense」(media.defense.gov)、2025 年 2 月 4 日にアクセス。

まとめ：レジリエンスには自動化と相互運用性が必要

大国間の競争で優位に立つために、国防総省の部隊には悪条件を予測し、それに耐え、そこから回復するための優れた能力が必要です。Red Hat と国防総省の取り組みについて詳細をご覧ください。

Red Hat について

Red Hat は、受賞歴のあるサポート、トレーニング、コンサルティング・サービスをお客様に提供し、複数の環境にわたる標準化、クラウドネイティブ・アプリケーションの開発、複雑な環境の統合、自動化、セキュリティ保護、運用管理を支援します。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com
#1666167_0225