

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
統治 (GV)	組織のサイバーセキュリティリスクマネジメント戦略、期待事項、および方針が確立され、伝達され、監視される			
組織的状況 (GV.OC)	組織のサイバーセキュリティリスクマネジメントに関する意思決定を取り巻く状況（使命、利害関係者の期待、依存関係、法的・規制的・契約上の要件）が理解されている			
GV.OC-01: 組織の使命が理解され、サイバーセキュリティリスクマネジメントに反映されている	<p><b>一般的な考慮事項：</b>一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b>NIST SP 800-53、改訂 5 版：PM-11</p>	<p><b>提案優先度：</b>3</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>OWASP AI Exchange：ガバナンス統制；OWASP LLM トップ 10：LLM03 サプライチェーン</p>	<p><b>提案優先度：</b>3</p> <p><b>機会例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>ENISA 脅威状況 2025；DASF 50；ATLAS AML.M0020；OWASP AI Exchange: AI Security Overview_ <a href="https://arxiv.org/pdf/2311.05232">https://arxiv.org/pdf/2311.05232</a>；NIST AI 100-2e2025</p>	<p><b>提案優先度：</b>3</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>AI 固有の参考情報例は追加情報待ち。</p>
GV.OC-02: 内部および外部の利害関係者を把握し、サイバーセキュリティリスクマネジメントに関する彼らのニーズと期待を理解し考慮する	<p><b>一般的な考慮事項：</b>AI の利用は、法務、技術、調達/買収、ガバナンスチームなど、組織運営の多面的な側面からの考慮事項をもたらす。これらの領域間の連携は、AI 関連のサイバーセキュリティリスクに対処するために不可欠である。</p> <p>学際的なアプローチは、包括的なエンタープライズ視点の構築を容易にする。</p>	<p><b>提案優先度：</b>3</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>DASF 13、40、51、53；OWASP AI Exchange：一般ガバナンス統制；OWASP LLM トップ 10：LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>サイバー防衛における AI 能力の強みと限界を理解することは、関係者の期待に応え、必要な人的監視と自動化のバランスを確保するために重要である。</p> <p><b>参考情報例：</b>DASF 38,50；OWASP AI Exchange: AI Transparency；ENISA 脅威状況 2025；ATLAS AML.M0003</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>AI 固有の参考情報例は追加情報待ち。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	<p><b>参考情報例：</b> NIST SP 800-53 第 5 版：PM-09；PM-18；PM-30；SR-03；SR-05；SR-06；SR-08；<a href="#">第 1 回サイバーAI プロファイルワークショップの考察</a></p>			
<p><b>GV.OC-03：</b> サイバーセキュリティに関する法的、規制上、契約上の要件（プライバシー及び市民的自由の義務を含む）を理解し管理する</p>	<p><b>一般的な考慮事項：</b> AI に関する法的・規制・標準の状況は急速に変化しており、組織が AI をいつ、どのように使用するかという判断に影響を与える。組織は自らの責任を認識し続けるための措置を講じる必要がある。規制および法的コンプライアンスを維持するためには、人間の監視が求められる。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AC-01；AT-01；AU-01；CA-01；CM-01；CP-01；IA-01；IR-01；MA-01；MP-01；PE01；PL-01；PM-01；PS-01；PT-01；RA-01；SA-01；SC-01；SI-01；SR-01；PM-28；PT</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> AI 利用に関する法的枠組みは、特にサイバーセキュリティ、プライバシー、著作権物の公正利用、AI トレーニングなどの分野で進化している。</p> <p><b>参考情報例：</b> DASF 32, 40；OWASP AI Exchange：不要な動作の影響を制限する制御；OWASP 従来型ランタイム制御；OWASP AI Exchange：一般的なガバナンス制御；OWASP AI Exchange：モデルアクセス制御；OWASP GenAI セキュリティプロジェクト：監視；OWASP LLM トップ 10；LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 1</p> <p><b>AI の活用例：</b> AI 機能は、法的・規制・契約上の要件を分析・要約し、ポリシー策定を加速し、レビュープロセスを迅速化し、文書間の類似概念を特定・マッピングすることで、法令遵守を支援できる。さらに自動化により、非準拠問題をリアルタイムで監視・識別・修正することで、監査プロセスを簡素化することさえ可能だ。</p> <p><b>重点領域の考慮事項例：</b> 防御型 AI ツールは、同意、利用、データ集約の制御、および新たな AI 特化法を含むプライバシー義務に沿ってログと機密データを扱う。</p> <p>AI 監査は、法的・規制的・契約上の要件への準拠を実証すると同時に、説明可能性といった AI 特有のニーズにも対応するよう設計されている。</p> <p><b>参考情報例：</b> DASF 44,50；ENISA 脅威状況 2025；ATLAS AML.M0005</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。</p>
<p><b>GV.OC-04：</b> 外部関係者が組織に依存または期待する重要な目的、能力、サービ</p>	<p><b>一般的な考慮事項：</b> AI がサイバーセキュリティに与える影響は管理されている。AI のサイバーセキュリティ能力と限界は理解さ</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> AI の意図された用途と既知の制限事項を伝えることは、効果的な利用に不可欠だ。AI がどのように意思決定を</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> 組織は、防御的意図決定支援や AI 検知を含む、ステークホルダーが依存する AI を活用したサイバーセキュリティ</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
スガ理解され、伝達される	れ、ユーザーに伝達されている。ガードレールとバックアップ計画が確立され、実施されている。  <b>参考情報例</b> : NIST SP 800-53, Rev 5: PM-08; PM-11; CP-02(08); PM-30(01); RA09	行うか、いつ誤りを犯すか、誤りを犯した際の対応策をユーザーに伝える必要がある。  <b>参考情報例</b> : DASF 11, 19, 40-42, 51, 53; OWASP AI Exchange: ガバナンス全般統制; OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	防御支援サービスを理解し、伝達する必要がある。  <b>参考情報例</b> : ENISA 脅威状況 2025 ; DASF 50 ; OWASP AI Exchange: Oversight ; ATLAS AML.M0008 ; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>参考情報例</b> : <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>
<b>GV.OC-05</b> : 組織が依存する成果、能力、サービスは理解され、伝達される	<b>一般的な考慮事項</b> : AI の出力は予測不可能である。システムの能力と限界は理解され、ユーザーに伝達されるガードレールとバックアップ計画が確立され、実施される。  <b>参考情報例</b> : NIST SP 800-53, Rev 5: PM-11; PM-30; RA-07; SA-09; SR-05	<b>提案優先度</b> : 1  <b>重点領域の考慮事項例</b> : 組織は AI システムに依存する業務成果を特定し、これらの依存関係を関連チームに明確に伝える。さらに、AI モデルの意図された用途と限界を理解することは、効果的な利用とサイバーセキュリティ対策に不可欠である。ユーザーは AI が意思決定を行う仕組み、誤りを発生した際の特定方法、誤り発生時の対応策を理解する必要がある。  <b>参考情報例</b> : DASF 23, 45, 51, 53 ; OWASP AI Exchange : 全般ガバナンス管理策 ; OWASP LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025 ; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>	<b>提案優先度</b> : 2  <b>重点領域の考慮事項例</b> : 組織は、防御機能のうち AI システムに依存するものを識別し、関連チームに対してこれらの用途と依存関係を明確に伝えるべきだ。敵対的操作、モデルドリフト、幻覚に対する AI 防御アクションを保護するため、HITL チェックと信頼閾値を用いて、AI 出力が行動に移すのに十分な信頼性があるかを示す。  <b>参考情報例</b> : OWASP AI Exchange: サプライチェーン管理 ; DASF 39,50 ; ATLAS AML.M0023 ; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>
<b>リスクマネジメント戦略 (GV.RM)</b>	組織の優先順位、制約、リスク許容度およびリスク選好に関する声明、ならびに前提条件が確立され、伝達され、業務上のリスク判断を支援するために使用される			
<b>GV.RM-01</b> : リスクマネジメント目標が設定	<b>一般的な考慮事項</b> : AI の利用がサイバーセキュリティリスクマネジ	<b>提案優先度</b> : 3	<b>提案優先度</b> : 2	<b>提案優先度</b> : 3

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
され、組織の利害関係者によって合意される	<p>メントの目標とどのように整合しているかを評価する。サイバーセキュリティリスクマネジメント目標を設定する際には、AI 固有の目標（例：誤検知率の低減、トリアージ速度の向上）を含めること。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版；PM-09；RA07；SR-02</p>	<p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> OWASP AI Exchange；ガバナンス全般統制；OWASP LLM Top Ten；LLM03 サプライチェーン ENISA 脅威状況 2025</p>	<p><b>機会例：</b> AI が脆弱性を分析し、早期警告を発する。インシデント発生前に防御策の優先順位付けを支援する。</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 50；ATLAS AML.M0000</p>	<p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<b>GV.RM-02:</b> リスク選好度およびリスク許容度の声明が確立され、伝達され、維持されている	<p><b>一般的な考慮事項：</b> 脅威と防御能力の進化する性質のため、AI に対するリスク許容度は頻繁に再評価する必要がある。</p> <p><b>参考情報例：</b> NIST SP 800-53 第 5 版；PM-09</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> AI 固有のリスクを組織の正式なリスク許容度および許容範囲の声明に統合する。AI システムの性質が進化するにつれて、リスク許容度および許容範囲を定期的に更新する。</p> <p><b>参考情報例：</b> OWASP AI Exchange；全般ガバナンス管理策；OWASP LLM トップ 10；LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> AI 固有のリスクを組織の正式なリスク許容度及び許容範囲の声明に統合する。AI システムの性質が進化するにつれ、リスク許容度及び許容範囲を定期的に更新する。</p> <p><b>参考情報例：</b> DASF 50；ENISA 脅威状況 2025；ATLAS AML.M0019</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> AI を活用した新たな脅威や攻撃の出現に伴い、リスク許容度の新たな推奨事項が必要となる可能性がある。</p> <p><b>参考情報例：</b> <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<b>GV.RM-03:</b> サイバーセキュリティリスクマネジメント活動とその成果は、エンタープライズリスクマネジメントプロセスに含まれる	<p><b>一般的な考慮事項：</b> AI リスクマネジメントを既存のエンタープライズリスクマネジメントの実践とガバナンス構造に統合する。</p> <p><b>参考情報例：</b> NIST SP 800-53 第 5 版；PM-03；PM-09；PM-30；RA-07；SA-24；SR-02；<a href="#">第 1 回サイバー</a></p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 5、13；OWASP AI Exchange；ガバナンス全般統制；OWASP LLM Top Ten；LLM03 サプライチェーン ENISA 脅威状況 2025；</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> AI セキュリティ脅威と AI 固有のセキュリティ対策（例：データ来歴証明追跡）の有効性が正式に報告され、組織のエンタープライズリスクマネジメントに組み込まれることを確保する。</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	<a href="#">AI プロファイルワークショップの考察</a>	<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	参考情報例：DASF 38,50；ENISA 脅威状況 2025；ATLAS AML.M0023； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	
<b>GV.RM-04:</b> 適切なリスク対応オプションを記述する戦略的方向性が確立され、伝達される	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版：PM-09；PM-28；PM-30；SR-02</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：OWASP AI Exchange：全般ガバナンス管理策；OWASP LLM トップ 10；LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p>提案優先度：3</p> <p>機会例：AI が脆弱性を分析し、早期警告を発する（）。また、インシデント発生前に防御策の優先順位付けを支援する。</p> <p>AI は複雑な技術データを明確なビジネス用語に変換する。技術的リスクを簡潔な洞察に要約し、経営陣が情報に基づいたリスク判断を下せるように支援する。</p> <p>重点領域の考慮事項例：プロンプト・インジェクション、モデル逆算、データ・ポイズニングなど、AI 固有のリスクに対応した具体的な戦略的リスク対応策（例：緩和、回避）を策定し、伝達する。</p> <p>参考情報例：OWASP AI Exchange: リスク Treatment; DASF 39; ENISA 脅威状況 2025; ATLAS AML.M0011; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>
<b>GV.RM-05:</b> サイバーセキュリティリスク（サプライヤーやその他のサードパーティからのリスクを含む）について、組織全体で情報伝達経路を確立する	<p>一般的な考慮事項：脅威ベクトルや防御能力に関する情報を共有するための AI 固有コミュニケーションチャンネルを構築する。</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：AI は急速に進化する分野であり、サイバーセキュリティリスクに関する頻繁な更新が必要となる可能性が高い。</p> <p>参考情報例：DASF 32, 51, 53; OWASP AI Exchange: ガバナンス全般統</p>	<p>提案優先度：2</p> <p>機会例：AI は標準プロトコル（STIX や OpenCTI など）を用いて脅威インテリジェンスをフォーマット化し共有し、チームやパートナー間の連携を維持する。</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：脆弱性管理が組織全体で伝達・実施されるよう確保し、AI を活用した攻撃に対処・エスカレーションするためのコミュニケーションチャンネルを構築する。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	<p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：PM-09；PM-30</p>	<p>制；OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>重点領域の考慮事項例：</b>リアルタイムのサイバーセキュリティインシデント発生時に、AI 駆動型ツールと人間のアナリストを迅速に共有・エスケーションするための専用コミュニケーションチャネルを構築する。</p> <p><b>参考情報例：</b> ENISA 脅威動向 2025；DASF 50；ATLAS AML.M0023</p>	<p><b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。</p>
<p><b>GV.RM-06：</b>サイバーセキュリティリスクの計算、文書化、分類、優先順位付けのための標準方法が確立され、コミュニケーションされる</p>	<p><b>一般的な考慮事項：</b>脅威と能力が進化するにつれ、組織のサイバーセキュリティリスク許容度を現在の状況に合わせて調整する。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：PM-09；PM-18；PM-28；PM-30；RA-03</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> AI システムは一般的に他の種類のソフトウェアよりも予測が困難である。予測不可能な行動の規模と範囲のため、AI リスクの計算、分類、優先順位付けの手法は、他の種類のソフトウェアを扱う方法とは異なる扱いを受ける。</p> <p><b>参考情報例：</b> OWASP AI Exchange: ガバナンス全般統制；OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> AI 特有の脅威（例：を識別し、対応する検知および制御メカニズムを統合する） モデル悪用、データ漏洩、新たなリスクなど）に対応する検知・制御メカニズムを統合し、未知または進化する攻撃パターンに適応する防御システムを確保する。</p> <p><b>参考情報例：</b> DASF 38、ATLAS AML.M0005、ENISA 脅威状況 2025、NIST AI 100-2e2025、 <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 脅威に関する知見は、リスク計算と優先順位付け規準の策定に資する。</p> <p><b>参考情報例：</b> <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<p><b>GV.RM-07：</b>戦略的機会（すなわち、ポジティブなリスク）は特徴づけられ、組織のサイバーセキュリティリスクに関する議論に含まれる</p>	<p><b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：PM-09；PM-18；PM-28；PM-30；RA-03</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> OWASP AI Exchange：全般ガバナンス管理策；OWASP LLM トップ 10：LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p>サイバー防衛活動における AI の活用を検討する際には、ポジティブなリスクを考慮に入れること。</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
			参考情報例：DASF 50；ENISA 脅威状況 2025	
<b>役割、責任、権限 (GV.RR)</b>	説明責任、業績評価、継続的改善を促進するためのサイバーセキュリティ上の役割、責任、権限を確立し、周知する			
<b>GV.RR-01:</b> 組織のリーダーシップはサイバーセキュリティリスクに対する責任と説明責任を負い、リスクを認識し、倫理的で、継続的に改善する文化を育む。	<p><b>一般的な考慮事項：</b>一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b>NIST SP 800-53、改訂 5 版：PM-02；PM-19；PM-23；PM-24；PM-29</p>	<p><b>提案優先度：</b>3</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>DASF 22；OWASP 従来型ランタイム制御；OWASP AI Exchange；モデルアクセス管理；OWASP LLM トップ 10；LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b>1</p> <p><b>機会例：</b>AI は複雑な技術データを明確なビジネス言語に変換する。具体的には技術的リスクを簡潔な知見に要約し、経営陣が迅速に情報に基づいたリスク判断を下せるように支援する。</p> <p><b>重点領域の考慮事項例：</b>サイバーセキュリティの責任者は、AI 機能がサイバーセキュリティプログラムのニーズをどのように支援できるかを評価し、AI によって生じる新たなリスクがサイバーセキュリティおよびエンタープライズリスク管理プロセスに組み込まれることを確保する。</p> <p>AI 駆動型防御行動と方針を承認・監督する組織リーダーを識別する。生成されたリスク記述の正確性と組織ニーズとの整合性を確認する。</p> <p><b>参考情報例：</b>DASF 50；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>AI リスクの進化する性質を常に認識し、新たなリスクを組織全体に周知する。</p> <p><b>参考情報例：</b>AI 固有の参考情報例は追加情報待ち。</p>
<b>GV.RR-02:</b> サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、伝達され、	<p><b>一般的な考慮事項：</b>AI システムの行動に対する責任は、人間に割り当てられている。</p> <p><b>参考情報例：</b>NIST SP 800-53 第 5 版：PM-02；PM-</p>	<p><b>提案優先度：</b>3</p> <p><b>重点領域の考慮事項例：</b>組織は自律システムによる行動の責任者を決定する。</p> <p><b>参考情報例：</b>DASF 19、22、36、41；OWASP 従来型ランタイム制御；OWASP</p>	<p><b>提案優先度：</b>1</p> <p><b>機会例：</b>AI エージェントは、ネットワークの監視、防御措置の妥当性確認、検知精度の向上を通じて、サイバーセキュリティ担当者を補強し、人的負担を軽減する可能性がある。</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>組織は、システムの防御とレジリエンスを強化するための役割と責任を人員に割り当てる。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
理解され、実施される	13 ; PM-19 ; PM-23 ; PM-24 ; PM-29	AI Exchange : モデルアクセス管理 ; OWASP LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>重点領域の考慮事項例 :</b> AI 駆動型防御行動 (例 : 自動ブロック) の責任範囲を定義し割り当てる。 <b>参考情報例 :</b> DASF 39,50 ; ATLAS AML.M0019 ; ATLAS AML.M0003 ; ENISA 脅威状況 2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>参考情報例 :</b> AI 固有の参考情報例は追加情報待ち。
<b>GV.RR-03:</b> サイバーセキュリティリスク戦略、役割、責任、方針に見合った十分なリソースが割り当てられている	<b>一般的な考慮事項 :</b> 担当者は、組織の AI システム管理ニーズを満たすために十分な認可とリソース (例 : 予算) を有している。AI システムの適切な使用と防御に関する担当者研修に十分なリソースが割り当てられている (PR.AT-01 および-02 も参照)。 <b>参考情報例 :</b> NIST SP 800-53、改訂 5 版 : PM-03	<b>提案優先度 :</b> 2 <b>重点領域の考慮事項例 :</b> 標準的なサイバーセキュリティ対策が適用される。 <b>参考情報例 :</b> AI 固有の参考情報例は追加情報待ち。	<b>提案優先度 :</b> 2 <b>機会例 :</b> 生産性や効率性などの向上を支援するため、人員にリソースが割り当てられる (例 : AI がアナリストの問題解決を支援する)。 <b>参考情報例 :</b> AI 固有の参考情報例は追加情報待ち。	<b>提案優先度 :</b> 1 <b>重点領域の考慮事項例 :</b> レジリエンスを強化し攻撃に耐えるための多層的アプローチを実現するリソースが利用可能である。 <b>参考情報例 :</b> AI 固有の参考情報例は追加情報待ち。
<b>GV.RR-04:</b> サイバーセキュリティは、人的資源管理の実践に組み込まれている	<b>一般的な考慮事項 :</b> AI システムを管理するにおける要員の役割、責任、スキルは明確に定義され文書化されている。これにより要員は AI がもたらす能力、限界、リスク、機会、影響、脅威を理解する。この情報は採用プロセス、要員管理、適切な役割に基	<b>提案優先度 :</b> 1 <b>重点領域の考慮事項例 :</b> AI モデルの限界を理解することは、効果的な使用に不可欠だ。その意思決定の仕組み、誤りを起こしやすい状況、そして誤りが発生した際の対応方法をユーザーに伝える方法を学ぶこと。 <b>参考情報例 :</b> DASF 33	<b>提案優先度 :</b> 3 <b>重点領域の考慮事項例 :</b> 標準的なサイバーセキュリティ対策が適用される。 <b>参考情報例 :</b> <a href="https://arxiv.org/html/2511.22189v1">https://arxiv.org/html/2511.22189v1</a>	<b>提案優先度 :</b> 1 脅威環境の変化速度は、AI を活用した攻撃によって加速する。チームが人員配置や訓練のニーズに対応するには、追加リソースが必要となる可能性が高い。 <b>参考情報例 :</b> <a href="https://arxiv.org/pdf/2305.06972">https://arxiv.org/pdf/2305.06972</a>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	<p>づく訓練に組み込まれるべきである (PR.AT-02 も参照)。</p> <p><b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : PM-13 ; PS01 ; PS-07 ; PS-09</p>			
<b>ポリシー (GV.PO)</b>	組織のサイバーセキュリティポリシーは確立され、周知され、実施される			
<b>GV.PO-01</b> : 組織の状況、サイバーセキュリティ戦略、優先事項に基づき、サイバーセキュリティリスクマネジメント方針を策定し、周知徹底および実施する	<p><b>一般的な考慮事項</b> : 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : AC-01 ; AT-01 ; AU-01 ; CA-01 ; CM-01 ; CP-01 ; IA-01 ; IR-01 ; MA-01 ; MP-01 ; PE01 ; PL-01 ; PM-01 ; PS-01 ; PT-01 ; RA-1 ; SA-01 ; SC-01 ; SI-01 ; SR-01</p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準のサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : OWASP AI Exchange : 望ましくない行動の影響を制限する制御 OWASP 従来型ランタイム制御 OWASP AI Exchange : 一般的なガバナンス制御 OWASP AI Exchange : モデルアクセス制御 OWASP GenAI セキュリティプロジェクト : 監視 OWASP LLM トップ 10 : LLM03 サプライチェーン ENISA 脅威状況 2025</p>	<p><b>提案優先度</b> : 1</p> <p><b>機会例</b> : AI が規制要件を分析し、監査と監査プロセスを簡素化し、現行の防御策が規制標準を満たしている箇所を正確に識別する。</p> <p><b>重点領域の考慮事項例</b> : AI を活用したサイバー防衛行動に関するルールを組み込む。これには、ガードレールの使用、透明性、HITL の妥当性確認と人間によるレビューのバランス、およびリスク判断前に の誤検知 (偽陰性・偽陽性) に対処するための人間によるレビューの重要性が含まれる。</p> <p><b>参考情報例</b> : DASF 50 ; ENISA 脅威状況 2025</p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : AI 固有の参考情報例は追加情報待ち。</p>
<b>GV.PO-02</b> : サイバーセキュリティリスクマネジメント方針は、要件、脅威、技術、組織の使命の変化を反映させるため、見直し、更新、コミュニケーション、実施される	<p><b>一般的な考慮事項</b> : AI 関連の方針をより頻繁に更新する。</p> <p><b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : AC-01 ; AT-01 ; AU-01 ; CA-01 ; CM-01 ; CP-01 ; IA-01 ; IR-01 ; MA-01 ; MP-01 ; PE-01 ; PL-01 ; PM-01 ; PS-</p>	<p><b>提案優先度</b> : 1</p> <p><b>重点領域の考慮事項例</b> : AI システムやその利用に関連する、あるいは影響を与える方針は、要件、脅威、技術的能力の急速な変化により、より頻繁な更新が必要となる場合がある。</p>	<p><b>提案優先度</b> : 1</p> <p><b>機会例</b> : AI はガバナンスチェックとして機能し、ポリシー要件を要約する (例 : 要件やルールと矛盾する防御行動をチェックしフラグを立てる)。</p> <p><b>重点領域の考慮事項例</b> : AI 脅威が急速に変化しているため、サイバーセキュリティリスクの</p>	<p><b>提案優先度</b> : 2</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : AI 固有の参考情報例は追加情報待ち。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	01 ; PT-01 ; RA-01; SA-01; SC-01; SI-01; SR-01	<b>参考情報例</b> : OWASP AI Exchange : 望ましくない行動の影響を制限する制御 ; OWASP 従来型ランタイム制御 ; OWASP AI Exchange : 一般的なガバナンス制御 ; OWASP AI Exchange : モデルアクセス制御 ; OWASP GenAI セキュリティプロジェクト : 監視 ; OWASP LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025	スクマネジメトポリシーのレビュー頻度を高めること。  <b>参考情報例</b> : ENISA 脅威状況 2025 ; OWASP AI Exchange: ガバナンス全般統制	
<b>監督 (GV.OV)</b>	組織全体のサイバーセキュリティリスクマネジメト活動と実績の結果は、リスクマネジメト戦略の策定、改善、調整に活用される			
<b>GV.OV-01:</b> サイバーセキュリティリスクマネジメト戦略の成果を検証し、戦略と方向性を情報提供・調整する	<b>一般的な考慮事項</b> : 防御システムの有効性と効果を判断するため、有害事象と防御対策の緩和を監視する。  <b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : AC-01 ; AT-01 ; AU-01 ; CA-01 ; CM-01 ; CP-01 ; IA-01 ; IR-01 ; MA-01 ; MP-01 ; PE01 ; PL-01 ; PM-01 ; PS-01 ; PT-01 ; RA-01 ; SA-01 ; SC-01 ; SI-01 ; SR-01 ; PM-09 ; PM-18 ; PM-30 ; PM-31 ; RA-07 ; SR-06	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : OWASP AI Exchange : 望ましくない行動の影響を制限する制御 ; OWASP 従来型ランタイム制御 ; OWASP AI Exchange : 一般的なガバナンス制御 ; OWASP AI Exchange : モデルアクセス制御 ; OWASP GenAI セキュリティプロジェクト : 監視 ; OWASP LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025	<b>提案優先度</b> : 2  <b>機会例</b> : AI はガバナンスチェックとして機能しポリシー要件を要約し、ルールと矛盾する防御的行動をチェックしてフラグを立てる。  <b>重点領域の考慮事項例</b> : AI 駆動型防御の成果を定期的に検証し、誤検知などの新たなリスクを導入せずに偽陽性 (FP) を削減しているか判断する  <b>参考情報例</b> : DASF 50 ; NIST AI 100-2e2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>提案優先度</b> : 2  <b>重点領域の考慮事項例</b> : AI を活用したインシデントからの検知、対応、復旧 管理が実行可能となるよう、必要に応じて使用を調整する。  <b>参考情報例</b> : NIST AI 100-2e2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>  AI 固有の参考情報例は追加情報待ち。
<b>GV.OV-02:</b> サイバーセキュリティリスクマネジメト戦略は、組織の要件とリスクを確実	<b>一般的な考慮事項</b> : リスクや機会が生じた際には、管理戦略を定期的に更新する。	<b>提案優先度</b> : 2  <b>重点領域の考慮事項例</b> : AI はリスクと機会の急速な変化に対応するため、サイバーセキュ	<b>提案優先度</b> : 2  <b>重点領域の考慮事項例</b> : 敵対的機械学習研究の知見や内部レッドチームテストの結果に	<b>提案優先度</b> : 2  <b>重点領域の考慮事項例</b> : AI を活用した戦術・技術から生じる新たな攻撃パターンには、急速に進化する技術的能力に対応するため、

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
にカバーするよう見直しと調整を行う。	<b>参考情報例：</b> NIST SP 800-53、改訂 5 版：PM-09；PM-19；PM-30；PM-31；RA-07；SR06	リテリスクマネジメント戦略の更新頻度を高める必要があるかもしれない。  <b>参考情報例：</b> OWASP AI Exchange：全般ガバナンス管理策；OWASP LLM トップ 10；LLM03 サプライチェーン；ENISA 脅威状況 2025	基づく新たな攻撃パターンに対応するため、更新頻度の向上が必要となる可能性がある。  <b>参考情報例：</b> ENISA 脅威状況 2025；OWASP AI Exchange：ガバナンス全般統制	新たな戦略とより緊密なフィードバックが必要となる可能性がある。  <b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。
<b>GV.OV-03:</b> 組織のサイバーセキュリティリスクマネジメントのパフォーマンスを評価し、必要な調整を検討する	<b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。  <b>参考情報例：</b> NIST SP 800-53、Rev 5：PM-04；PM-06；RA-07；SR-06	<b>提案優先度：</b> 3  <b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例：</b> OWASP AI Exchange：一般 ガバナンス管理；OWASP LLM トップ 10；LLM03 サプライチェーン	<b>提案優先度：</b> 2  <b>機会例：</b> AI は、明確なインシデント概要やコンプライアンス報告書のドラフト、証拠の整理、標準文書生成を通じて報告を支援し、アナリストの業務負荷を軽減する。AI 生成の報告書は、組織のリスクマネジメントに変更を加える前に、内容について人間（例：アナリスト）によるレビューを受けるべきである。  <b>重点領域の考慮事項例：</b> 精度、再現率、および人間の介入率を測定し、必要な調整を評価・検討する。  <b>参考情報例：</b> DASF 50；OWASP AI Exchange：モデル逆算とメンバーシップ推論；OWASP AI Exchange：不透明な信頼度；NIST AI 1002e2025	<b>提案優先度：</b> 3  <b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。
<b>サイバーセキュリティ・サプライチェーンリスクマネジメント (GV.SC)</b>	サイバーサプライチェーンリスクマネジメントプロセスは、組織の利害関係者によって特定、確立、管理、監視、改善される			
<b>GV.SC-01:</b> サイバーセキュリティサプライ	<b>一般的な考慮事項：</b> 組織は、AI コンポーネント（例：マイクロ	<b>提案優先度：</b> 2	<b>提案優先度：</b> 2	<b>提案優先度：</b> 2

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
チェーンリスクマネジメントプログラム、戦略、目標、方針、プロセスが確立され、組織の利害関係者によって合意される	<p>サービス、コンテナ、ライブラリ、データ、ハードウェアソフトウェア)の起源、それらが導入する可能性のある新たな脆弱性、およびサイバーセキュリティへの潜在的な影響を理解する必要がある。</p> <p><b>参考情報例</b> : NIST SP 800-53 第5版 : PM-30 ; SR-02 ; SR-03 ; <a href="#">第1回サイバーAI プロファイルワークショップ</a></p>	<p><b>重点領域の考慮事項例</b> : AIにおいては、データ来歴証明はソフトウェアやハードウェアの起源と同様に重視されるべきである。</p> <p>AIのサプライチェーンにおいて、全てのデータ入力(学習用と推論用の両方)は重要な要素だ。強化学習(RL)では、データは学習環境から得られる。モデルの環境条件( )がサプライチェーンリスクと整合していることに特に注意せよ。</p> <p><b>参考情報例</b> : DASF 22, 23, 32, 45, 51, 53; ATLAS AML.M0023; OWASP AI Exchange: AI 全般統制; OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025; AI 100-2e2025</p>	<p><b>重点領域の考慮事項例</b> : トレーニングデータと入力データの完全性(データ供給チェーンの一部)を検証し、データ・ポイズニングや改ざんを検知・防止すべきである。</p> <p>一部の組織では、RLを用いてネットワーク上の悪意ある活動を検知できる。例えば、オンライン学習を用いるモデルは日々の活動から絶えず改善される。悪意ある攻撃者は、ネットワークを正常に稼働させたまま、モデルのシステムを誤作動させる方法を編み出す可能性がある。時間が経つにつれ、モデルはこの行動が誤警報を引き起こすと「学習」し、将来この行動が発生してもオペレーターに警告しなくなるかもしれない。これを防御するには、モデルの訓練方法を慎重に検討する必要がある(つまり、オンライン訓練を許可しない、または妥当性確認データセットを使用しないこと)。</p> <p><b>参考情報例</b> : ENISA 脅威状況 2025 ; NIST AI 100-2e2025</p>	<p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。(理由) 内部データ、システム、ソフトウェアへのアクセス権を持つサプライヤーやサードパーティが、AIを活用したサイバー攻撃の標的となる可能性がある。</p> <p><b>参考情報例</b> : NIST SP 800-161 Rev. 1 ; AI 1002e2025</p>
<b>GV.SC-02:</b> サプライヤー、顧客、パートナーのサイバーセキュリティにおける役割と責任が確立され、社内外で伝達・調整される	<p><b>一般的な考慮事項</b> : AIコンポーネントの透明性と説明責任を高めるためのAIソフトウェア部品表(AI SBOM)の使用。</p> <p><b>参考情報例</b> : NIST SP 800-53 第5版 : SR-02 ; SR-03 ; SR-05 ; <a href="#">第1回サイバーAI プロファイルワークショップの考察</a></p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : DASF 32 ; ATLAS AML.M0023 ; OWASP AI Exchange : ガバナンス全般統制 ; OWASP LLM Top Ten : LLM03 サプライチェーン ENISA 脅威状況 2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : DASF 39 ; ENISA 脅威状況 2025</p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : NIST SP 800-161 Rev. 1 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<b>GV.SC-03:</b> サイバーセキュリティ サプライチェーンリスクマネジメントは、サイバーセキュリティおよびエンタープライズリスクマネジメント、リスクアセスメント、改善プロセスに統合されている	<b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。 <b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AC-01；AT-01；AU-01；；CA-01；CM-01；CP-01；IA-01；IR-01；MA-01；MP-01；PE01；PL-01；PM-01；PS-01；PT-01；RA-01；SA-01；SC-01；SI-01；SR-01；PM-09；PM-18；PM-30；PM-31；SR02；SR-03；RA-03；RA-07	<b>提案優先度：</b> 1 <b>重点領域の考慮事項例：</b> AI ソフトウェアを検討する際、サプライチェーンリスクマネジメントのためのサイバーセキュリティ対策は従来通りである。ただし、データが AI システムの運用において重要な役割を果たす点も考慮すべきだ。ソフトウェアのサプライチェーンと同様の重要性をもって扱う必要がある。 <b>参考情報例：</b> DASF 13、22、23、45、51、53；OWASP AI Exchange: 不要な動作の影響を制限する制御；OWASP 従来型ランタイム制御；OWASP AI Exchange: 一般的なガバナンス制御；OWASP AI Exchange: モデルアクセス制御；OWASP GenAI セキュリティプロジェクト: 監視；OWASP LLM トップ 10: LLM03 サプライチェーン；ENISA 脅威状況 2025；AI 100-2e2025	<b>提案優先度：</b> 2 <b>重点領域の考慮事項例：</b> サイバーセキュリティのサプライチェーンリスクマネジメントに AI 関連のリスク考慮事項を統合し、モデルの侵害やデータセットの汚染による防御能力の弱体化を防ぐ。 <b>参考情報例：</b> ENISA 脅威動向 2025；DASF 38,50；ENISA 脅威動向 2025；AI 100-2e2025	<b>提案優先度：</b> 3 <b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。 <b>参考情報例：</b> NIST SP 800-161 Rev. 1
<b>GV.SC-04:</b> サプライヤーは特定され、重要度に応じて優先順位付けされる	<b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。 <b>参考情報例：</b> NIST SP 800-53、改訂 5 版：RA-09；SA-09；SR-06	<b>提案優先度：</b> 2 <b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。(理由) AI ベースのサービスは、データ、計算インフラ、ソフトウェア、モデル、推論エンドポイントにおいてサプライヤーへの依存度を高める。この依存度の高まりは、サプライヤーを把握することの重要性を増す。ただし、サプライヤーを識別し優先順位を付ける方法は変わらない。	<b>提案優先度：</b> 3 <b>重点領域の考慮事項例：</b> サイバーセキュリティ防御に用いる AI モデルを、侵害された場合の潜在的な悪影響に応じてランク付けする。これにより防御措置の効果的な優先順位付けが可能となる。 <b>参考情報例：</b> DASF 50；ENISA 脅威状況 2025	<b>提案優先度：</b> 3 <b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。 <b>参考情報例：</b> NIST SP 800-161 Rev. 1

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		<p><b>参考情報例：</b> DASF 13、23、32、45；ATLAS AML.M0023；OWASP AI Exchange：全般ガバナンス管理策；OWASP LLM トップ 10：LLM03 サプライチェーン；ENISA 脅威状況 2025</p>		
<p><b>GV.SC-05：</b> サプライチェーンにおけるサイバーセキュリティリスクに対処するための要件を確立し、優先順位付けを行い、サプライヤーやその他の関連するサードパーティとの契約やその他の合意に組み込むこと</p>	<p><b>一般的な考慮事項：</b> 標準のサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> NIST SP 800-53 Rev. 5：SA-04；SA-09；SR-03；SR-05；SR-06；SR-10</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。(理由) AI システムは、ほとんどのソフトウェアシステムよりもサプライチェーンが長い(例：サードパーティ製ハードウェアやコンピューティングインフラへの依存度が高い)。これらの要件を確立することは重要だが、その方法は他の種類のソフトウェアと同様である。</p> <p>例えば、AI システムは他のソフトウェアよりも、より意味のある形でトレーニングデータに依存する傾向がある。その結果、組織はソフトウェアやハードウェアだけでなく、データについてもサプライチェーンを考慮するようになる。</p> <p><b>参考情報例：</b> DASF 19、22、41、51、53；ATLAS AML.M0023；OWASP AI Exchange：ガバナンス全般統制；OWASP LLM Top Ten：LLM03 サプライチェーン ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> ベンダーに対し、AI ツールのモデル範囲とデータ範囲、ならびにインシデント対応の開示を義務付ける。</p> <p><b>参考情報例：</b> DASF 39,50；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> NIST SP 800-161 Rev. 1</p>
<p><b>GV.SC-06：</b> 正式なサプライヤーその他のサードパーティとの関係を結ぶ前に、リスクを低</p>	<p><b>一般的な考慮事項：</b> サードパーティサプライヤーがこれらのモデルを作成する際、自らデューデリジェンスを実施していることを確認す</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> サードパーティとの関係を結ぶ前に、サプライヤーの信頼性、デー</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> サードパーティの AI ソリューションを採用する前に、AI に特化したデューデリジェンスと敵対的テストを実施し、モ</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
減するための計画とデューデリジェンスを実施する	<p>ること。これには、モデルを自社内で作成する場合に考慮される全ての要素が含まれる。サプライヤーが使用するモデル訓練手法及び入力 データが、アクセス可能かつ透明性のあるものであることを確認すること。</p> <p><b>参考情報例：</b> NIST SP 800-53 第 5 版：SA-04；SA-09；SR-05；SR-06</p>	<p>タの透明性、およびトレーニングと評価方法を検討する。</p> <p><b>参考情報例：</b> DASF 22、51、53；DASF 51；ATLAS AML.M0023；OWASP AI Exchange：ガバナンス全般統制；OWASP LLM Top Ten：LLM03 サプライチェーン ENISA 脅威状況 2025</p>	<p>デルの脆弱性、倫理的整合性、およびパフォーマンスへの影響を評価する。</p> <p><b>参考情報例：</b> DASF 39,50；ENISA 脅威状況 2025</p>	<p><b>参考情報例：</b> NIST SP 800-161 Rev. 1</p>
<p><b>GV.SC-07:</b> 取引先、その製品・サービス、およびその他のサードパーティがもたらすリスクは、取引関係を通じて理解され、記録され、優先順位付けされ、アセスメントされ、対応され、監視される</p>	<p><b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：RA-09；SA-04；SA-09；SR-03；SR-06</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。(理由) これらのリスクへの対処方法は、システムが AI 対応か否かにかかわらずほぼ同じだが、極めて重要な検討事項であることに変わりはない。</p> <p><b>参考情報例：</b> DASF 7, 12, 14, 19, 29, 32, 35-39; DASF 41-42, 46, 52; 55; ATLAS AML.M0023; OWASP AI Exchange: AI 全般統制; OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025; AI 100-2e2025</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> サプライヤープロバイダによる AI モデル、データセット、API 全体に継続的な監視と脅威検知を実施し、サプライヤーに起因する敵対的行為、データ漏洩、または侵害されたコンポーネントを識別する。</p> <p><b>参考情報例：</b> DASF 38,39,50; ENISA 脅威状況 2025; AI 100-2e2025</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> NIST SP 800-161 Rev. 1</p>
<p><b>GV.SC-08:</b> 関連するサプライヤー及びその他のサードパーティは、インシデント計画、対応、復旧活動に含まれる</p>	<p><b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b> NIST SP 800-53、Rev 5：SA-04；</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。(理由) AI 環境においてもサプライヤーとの連携方法は変わらないが、こうした関係を構築する重要性は依然として高い。</p>	<p><b>提案優先度：</b> 3</p> <p><b>機会例：</b> AI は標準プロトコル (STIX や OpenCTI など) を用いて脅威インテリジェンスを収集・フォーマット・共有し、チームやパートナー間の連携を保証する。</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。(理由) エンドポイント検知サービスなど、サイバー防御を強化するためにサードパーティ供給業者を通じて防御対策に AI が統合される場合、組織はイ</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	SA09 ; SR-02 ; SR-03 ; SR-08 ; CP-01 ; IR01	<b>参考情報例</b> : DASF 23、39、45 ; ATLAS AML.M0023 ; OWASP AI Exchange : 全般ガバナンス Controls ; OWASP LLM Top Ten ; LLM03 サプライチェーン ENISA 脅威状況 2025	<b>重点領域の考慮事項例</b> : AI モデルやデータを提供するサプライヤーやパートナーを、AI 固有のインシデント対応・復旧計画に統合する。特に敵対的攻撃やデータ・ポイズニングの協同的検知に焦点を当てる。  <b>参考情報例</b> : DASF 39 ; ENISA 脅威状況 2025	インシデント対応計画に 供給業者を含めることが重要である。  <b>参考情報例</b> : NIST SP 800-161 Rev. 1
<b>GV.SC-09:</b> サプライチェーンのセキュリティ対策は、サイバーセキュリティおよびエンタープライズリスクマネジメントプログラムに統合され、そのパフォーマンスは技術製品およびサービスのライフサイクル全体を通じて監視される	<b>一般的な考慮事項</b> : 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。  <b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : PM-09 ; PM-19 ; PM-28 ; PM-30 ; PM-31 ; RA-03 ; RA-07 ; SA-04 ; SA-09 ; SR02 ; SR-03 ; SR-05 ; SR-06	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : DASF 23、45、51、53 ; ATLAS AML.M0023 ; OWASP AI Exchange : ガバナンス統制 ; OWASP LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : DASF 38,50 ; ENISA 脅威状況 2025	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : NIST SP 800-161 Rev. 1
<b>GV.SC-10:</b> サイバーセキュリティのサプライチェーンリスクマネジメント計画には、パートナーシップ契約やサービス契約の終了後に発生する活動に関する規定を含めること。	<b>一般的な考慮事項</b> : サードパーティのリソースを利用する前に、AI に関する利用規約 (例 : データ所有権、許容されるデータ利用方法) を確認し理解すること。  <b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : PM-31 ; RA-03 ; RA-05 ; ; RA-07 ; SA-04 ; SA-09 ; SR-02 ; SR-03 ; SR-05 ; SR-06	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : DASF 13、51、53 ; ATLAS AML.M0023 ; OWASP AI Exchange : 全般ガバナンス管理策 ; OWASP LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : DASF 39 ; ENISA 脅威状況 2025	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : NIST SP 800-161 Rev. 1

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
識別 (ID)	組織の現在のサイバーセキュリティリスクは把握されている			
資産管理 (ID.AM)	組織が事業目的を達成するために活用する資産（例：データ、ハードウェア、ソフトウェア、システム、施設、サービス、人材）は、組織目標に対する相対的重要性と組織のリスク戦略に基づき、識別され管理される			
<b>ID.AM-01</b> ：組織が管理するハードウェアの在庫リストを維持する	<b>一般的な考慮事項</b> ：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。  <b>参考情報例</b> ：NIST SP 800-53、改訂 5 版：CM-08；PM05	<b>提案優先度</b> ：3  <b>重点領域の考慮事項例</b> ：標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> ：DASF 10-11、18-19、29、34；ENISA 脅威状況 2025	<b>提案優先度</b> ：2  <b>重点領域の考慮事項例</b> ：AI を活用したサイバー防御に用いられる高速コンピューティングリソースを把握する。これらの資産を追跡することで、防御・運用に必要な十分な計算能力を確保し、インシデント対応時の迅速な範囲特定と封じ込めを支援する。  <b>参考情報例</b> ：DASF 1,34；ATLAS AML.M0023；ENISA 脅威状況 2025	<b>提案優先度</b> ：3  <b>重点領域の考慮事項例</b> ：標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> ：NIST SP 800-172 構成管理 3.4.1e-3.4.3e；
<b>ID.AM-02</b> ：組織が管理するソフトウェア、サービス、システムのインベントリを維持する	<b>一般的な考慮事項</b> ：AI 機能は既存システムに組み込まれるケースが増加しており、最新のインベントリ維持に課題が生じる可能性がある。  <b>参考情報例</b> ：NIST SP 800-53、Rev 5：AC-20；CM-08；PM-05；SA-05；SA-09	<b>提案優先度</b> ：2  <b>重点領域の考慮事項例</b> ：標準的なサイバーセキュリティ対策が適用される。（理由）組み込み AI 機能を有するシステムを識別することは、特にサードパーティから購入したシステムの場合、必ずしも容易ではない。  <b>参考情報例</b> ：DASF 10-11、18-19、23、29-30、32、34、45、48；OWASP AI Exchange: 不要な動作の影響を制限する制御；OWASP 従来型ランタイム制御；OWASP AI Exchange: 一般的なガバナンス制御；OWASP AI Exchange: モデルアクセス制御；OWASP LLM トップ 10: LLM03 サプライチェーン；ENISA 脅威状況 2025	<b>提案優先度</b> ：2  <b>重点領域の考慮事項例</b> ：インベントリには AI モデル、API、キー、エージェント、データ（ID.AM07 も参照）、およびそれらの統合と権限を含めるべきだ。  <b>参考情報例</b> ：DASF 39,50；ENISA 脅威状況 2025；AI 100-2e2025	<b>提案優先度</b> ：3  <b>重点領域の考慮事項例</b> ：標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> ：NTIA SBOM（全編）；NIST SP 800-172 構成管理 3.4.1e-3.4.3e；NIST SP 800-218（全編）；ATT&CK M1047

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<b>ID.AM-03:</b> 組織の認可されたネットワークコミュニケーションおよび内部・外部ネットワークデータフローの表現が維持されている	<p><b>一般的な考慮事項:</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例:</b> NIST SP 800-53、改訂 5 版: AC-04; CA-03; CA-09; PL-02; PL-08; PM-07</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> トラフィックを 4 つの明確なグループに分類する。内部の人間生成トラフィック、内部のコンピューター生成ネットワークトラフィック (cron ジョブや自動化プロセスなど)、内部の AI ベーストラフィック (ウェブ検索や組織リソースを利用する AI ツール)、外部トラフィックである。</p> <p>外部トラフィックは人間かボットか判別が難しいことに注意せよ。ただし、モデルレジストリやデータセットソース周辺のネットワークトラフィックを追跡することは、サプライチェーン攻撃の試みをより効果的に検知する上で価値がある。</p> <p><b>参考情報例:</b> DASF 5、7、10-11、13、16、18-19、24、28、30-32、41、44、48、52、56、58-60、62; OWASP AI Exchange: 望ましくない行動の影響を制限する制御; OWASP 従来型ランタイム制御; OWASP AI Exchange: 一般的なガバナンス制御; OWASP AI Exchange: モデルアクセス制御; OWASP LLM トップ 10: LLM03 サプライチェーン; ENISA 脅威状況 2025</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AI データフローの可視化を維持する。これには推論リクエストの経路やトレーニングデータパイプラインを含み、防御境界の強制と異常検知を可能とする。</p> <p><b>参考情報例:</b> DASF 38; ENISA 脅威状況 2025; AI 100-2e2025</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。ネットワークを理解することで、セキュリティイベントの発生を示す正常・異常トラフィックの判別が容易になる。</p> <p><b>参考情報例:</b> NIST SP 800-172 構成管理 3.4.1e-3.4.3e; ATT&amp;CK M1015; ATT&amp;CK M1028; AI 100-2e2025</p>
<b>ID.AM-04:</b> サプライヤーがプロバイダとして提供するサービスのインベントリは維持される	<p><b>一般的な考慮事項:</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。(理由) サードパーティサービスの棚卸しは重要だが、その手法は AI の文脈でも変わらない。</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> サプライヤーがプロバイダとして提供する外部 AI 防御コンポーネントおよびサービス (例: 検知モデル) は、サービスインベントリに記載すべきである。</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。最新の資産台帳により、AI を活用した攻撃の影響を受ける可能性のある、あるいはその原因となるサプライ</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	<p>参考情報例：NIST SP 800-53、改訂 5 版：AC-20；SA-09；SR-02</p>	<p>参考情報例：DASF 2、5、18、23-24、29、32-33、42、45、48、64；OWASP AI Exchange：不要な動作の影響を制限する制御；OWASP 従来型ランタイム制御；OWASP AI Exchange：一般的なガバナンス制御；OWASP AI Exchange：モデルアクセス制御；OWASP LLM トップ 10：LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p>参考情報例：DASF 45,48；ATLAS AML.M0005；ENISA 脅威状況 2025</p>	<p>ヤーやサードパーティがプロバイダとなるサービスの追跡と管理が可能となる。</p> <p>参考情報例：ATLAS AML.M0023；NTIA SBOM (全)；NIST SP 800-218 (全)；ATT&amp;CK M1033；AI 100-2e2025</p>
<p><b>ID.AM-05:</b> 資産は分類、重要度、リソース、および任務への影響に基づいて優先順位が付けられる</p>	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版：RA-03；RA-09；RA-02</p>	<p>提案優先度：2</p> <p><b>重点領域の考慮事項例：</b>新規</p> <p>AI システムには分類が必要となる。これらのシステムはまた、他の ソフトウェアシステムが通常影響を受けない方法で、システムの機能性と脆弱性に直接寄与するリソース（例えばトレーニングデータセット）を消費し使用する。</p> <p>参考情報例：DASF 5-6、23-24、30、45；OWASP AI Exchange：AI ガバナンス Controls；OWASP LLM Top Ten：LLM03 サプライチェーン ENISA 脅威状況 2025</p>	<p>提案優先度：3</p> <p><b>重点領域の考慮事項例：</b>AI 資産（例：モデル、推論サービス）を、重要度、任務への影響度、および AI を活用した防御におけるデータ格付に基づいて優先順位付けする。</p> <p>参考情報例：DASF 38；ENISA 脅威動向 2025</p>	<p>提案優先度：3 <b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>
<p><b>ID.AM-07:</b> 指定データおよび対応するメタデータのインベントリデータタイプに対応するデータとメタデータのインベントリを維持する</p>	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版：CM-12；CM13；SI-12</p>	<p>提案優先度：1</p> <p><b>重点領域の考慮事項例：</b>データプロビネンスとデータインベントリは、データとメタデータの性質、およびそれらに付随する要件（利用契約や同意など）を理解する上で相互に補完的な役割を果たす。これにより、外部ソースから収集されたデータや共有されるデータ（外部だけでなく、異なる目的で内部共有される場合</p>	<p>提案優先度：1</p> <p>AI 技術は、組織が管理するデータとメタデータをより迅速に理解する能力を強化する。具体的には、ネットワーク上の所在場所の特定、データの性質の把握、コンプライアンスやその他のリスクマネジメント要件との整合性確保（例：法令や規制による保護対象となるデータの識別）などが含まれる。</p>	<p>提案優先度：3</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：AI 100-2e2025</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		<p>も含む) については、追加的な注意が必要となる場合がある。NIST プライバシーフレームワークを適用することで、組織がプライバシーリスクを管理するのに役立つ。</p> <p>機械学習に使用されるデータの全体像を把握するには、新たなメタデータの追跡が必要となる。例えば、モデルを訓練するためにどのようなメモリ内データ変換/拡張が行われているのか? AI データセットの来歴証明を維持せよ。変更されたデータはデータ・ポイズニングが発生した可能性を示す。組織外から調達した訓練データは追加の不確実性を生じさせる。</p> <p><b>参考情報例</b> : DASF 5-6、10-11、15、17、21、30、32、48、56、58-59、62 ; ENISA 脅威状況 2025 ; AI 1002e2025</p>	<p><b>重点領域の考慮事項例</b> : データとその対応するメタデータ (例 : 保存場所、必要な保護措置) を理解することは、効果的な AI を活用した防御にとって重要だ。AI はデータの自動発見、ラベル付けと分類、特別な処理が必要な情報の識別を支援できる。</p> <p><b>参考情報例</b> : DASF 5,38; ENISA 脅威状況 2025; AI 100-2e2025</p>	
<p><b>ID.AM-08</b>: システム、ハードウェア、ソフトウェア、サービス、データは、そのライフサイクル全体を通じて管理される。</p>	<p>一般的な考慮事項 : 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : CM-09 ; CM-13 ; MA-02 ; MA-06 ; PL-02 ; PM-22 ; PM-23 ; SA-03 ; SA-04 ; SA-08 ; SA-22 ; SI-12 ; SI-18 ; SR-05 ; SR-12</p>	<p><b>提案優先度</b> : 1</p> <p><b>重点領域の考慮事項例</b> : データは AI ベースシステムの性能において特に重要な役割を果たす。自動的な意思決定を行うシステムや、他のプロセス (例 : トレーニングデータ) にデータを提供するシステムにおいては、データとシステムのライフサイクル全体を通じてデータ品質を確保することが特に重要である。これにより、誤りや「不良」データが拡散するのを防ぐことができる。</p> <p><b>参考情報例</b> : DASF 6-7、10-12、14、16-20、22-23、29-30、32、34、38、41-42、48、52、59、63 ; OWASP 従来型ランタイム制御; OWASP AI Exchange: ー</p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : DASF 6,38,50; ENISA 脅威状況 2025; AI 100-2e2025</p>	<p><b>提案優先度</b> : 2</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。(根拠) システムのライフサイクル全体を通じた維持管理は、AI を活用した攻撃が古いコンポーネントや管理不行き届きのコンポーネントを新たな攻撃対象として利用しようとする場合に、レジリエンスを高め効果性を確保する。</p> <p><b>参考情報例</b> : NIST SP 800-281 (全編) ; NTIA SBOM (全編) ; ATLAS AML.M0023 ; ATT&amp;CK M1054 ; AI 100-2e2025</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		<p>一般的なガバナンス制御; OWASP AI Exchange: モデルアクセス管理; OWASP モデル入力機密性; OWASP LLM トップ 10: LLM03 サプライチェーン; ENISA 脅威状況 2025; AI 100-2e2025</p>		
<b>リスクアセスメント (ID.RA)</b>	組織、資産、個人に対するサイバーセキュリティリスクは、組織によって理解されている			
<b>ID.RA-01: 資産の脆弱性を識別し、を妥当性確認し、記録する</b>	<p><b>一般的な考慮事項:</b> AI は新たな種類の脆弱性（敵対的入力など）をもたらす。組織は AI アプリケーションのセキュリティ確保や、組織防衛のための AI システム利用時にこれらを考慮する必要がある。</p> <p>AI システムはソフトウェアの既存の脆弱性も悪用し得る。</p> <p><b>参考情報例:</b> NIST SP 800-53, Rev 5 : CA-02, CA-07, CA-08, RA-03, RA-05, SA11(02), SA-15(07), SA-15(08), SI04, SI-05</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> AI には敵対的入力など、新たな種類の脆弱性が存在する。これにより、識別・追跡・記録すべき新たな脆弱性の群が生じる。</p> <p><b>参考情報例:</b> DASF 13, 16, 19, 22-23, 31-32, 36, 38, 41-42, 45-46, 52-53, 56, 63 ; OWASP 標準実行時制御 ; OWASP 基本 ; <a href="https://arxiv.org/pdf/2409.08831_v1">https://arxiv.org/pdf/2409.08831_v1</a> ; ガバナンス; OWASP GenAI セキュリティプロジェクト : 監視; OWASP LLM トップ 10 : LLM03 サプライチェーン; ENISA 脅威状況 2025; <a href="https://arxiv.org/pdf/2504.11168">https://arxiv.org/pdf/2504.11168</a>; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>; AI 100-2e2025</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 脆弱性管理に AI 固有攻撃（例：敵対的入力、モデル回避）を含め、最近の脅威レポートに記載された AI を活用した攻撃をフラグ付けし、防御策が最新であることを確保する。</p> <p><b>参考情報例:</b> DASF 38,39; ENISA 脅威状況 2025; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>; <a href="https://arxiv.org/pdf/2409.08831v1">https://arxiv.org/pdf/2409.08831v1</a>; AI 100-2e2025</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> ソフトウェアなどの資産の脆弱性は、AI を活用した攻撃によって悪用される可能性があるため、従来のサイバーセキュリティ対策よりも迅速な特定と解決が必要となる。</p> <p><b>参考情報例:</b> NIST SP 800-218 (全編) ; NTIA SBOM (全編) ; ATLAS AML.M0016 ; ATT&amp;CK M1016 ; ATT&amp;CK M1051 ; <a href="https://arxiv.org/pdf/2504.11168">https://arxiv.org/pdf/2504.11168</a>; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<b>ID.RA-02: サイバー脅威インテリジェンスは情報共有フォーラムや情報源から入手される</b>	<p><b>一般的な考慮事項:</b> AI 関連の新たな情報共有源を取り入れること。具体的には、出版物、学術や情報源から入手される</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> モデルに即座に現実世界への影響を与え得る情報は、AI 学術出版物から得られる場合がある。例えば、AI 脱獄やプロンプト・インジェクション技術は、他の</p>	<p><b>提案優先度:</b> 2</p> <p><b>機会例:</b> AI は防御側に、膨大なデータセットをスキャンし、大量の脅威インテリジェンスを迅速に分析し、複数の情報源からのデータを相関さ</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。（理由）レッドチーム活動や侵入テスト演習からの情報、ならびに AI 関連の学術論文を活用し、AI を活用</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	誌、ISAC/ISAO、 <sup>1</sup> 、その他のフォーラムからの AI 固有脅威インテリジェンスなどである。利用可能なリソースの例としては、OWASP <sup>7</sup> 、 <a href="#">AI インシデントデータベース (AIID)</a> 、 <a href="#">MITRE ATLAS™</a> が挙げられる。  <b>参考情報例：</b> NIST SP 800-53 Rev 5 : SI-05 ; PM15 ; PM-16	サイバーセキュリティ情報源と比較して、AI 関連ジャーナルで発見・発表される可能性が高い。  <b>参考情報例：</b> ENISA 脅威動向レポート 2025	せることで支援する。これにより防御側は脅威の状況を明確かつ予測可能な形で把握できる。  <b>重点領域の考慮事項例：</b> の研究や業界共有リソース（例：ATLAS™）から、脱獄やプロンプト・インジェクションなどの AI 関連 CTI を取得する。  <b>参考情報例：</b> DASF 39 ; ENISA 脅威状況 2025	した攻撃を阻止する将来の能力構築に役立つべきである。  <b>参考情報例：</b> <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>
<b>ID.RA-03:</b> 組織に対する内部および外部の脅威を識別し記録する	<b>一般的な考察：</b> AI は組織に対して数多くの新たな内部・外部脅威をもたらすが、同時にこれらの脅威に対抗する機会も提供する。  <b>参考情報例：</b> NIST SP 800-53 第 5 版 : PM-12 ; PM16 ; RA-03 ; SI-05	<b>提案優先度：</b> 1  <b>重点領域の考慮事項例：</b> LLM ベースのシステムは自律的に動作し、計算環境内で任意のコードを実行する能力が与えられる場合がある。自律的な動作に伴う潜在的な不確実性（例：コード実行への操作）は、他の脅威と併せて考慮すべきである。  AI システムは完全に予測可能ではない。これらのシステムは、学習領域外の入力に対して予期せぬ出力を示す可能性がある。  <b>参考情報例：</b> DASF 13, 32; OWASP AI Exchange: 一般的なガバナンス管理策; OWASP LLM トップ 10: LLM03 サプライチ	<b>提案優先度：</b> 1  <b>機会例：</b> AI は異常をフラグ付けし、不審な行動を相関させ、他のツールより迅速に異常パターンを検知することで、監視を改善し脅威検知を強化する。  AI は防御側を支援する。膨大なデータセットをスキャンし、大量の脅威インテリジェンスを迅速に分析することで、IT、OT、IoT にまたがる内部・外部脅威を識別し、防御側に脅威の全体像を明確に示すのだ。  <b>重点領域の考慮事項例：</b> 防御システムを直接標的とする、あるいは欺く可能性のある内部・外部の AI 活用型脅威（AI 活用型フィッシン	<b>提案優先度：</b> 1  <b>重点領域の考慮事項例：</b> AI を活用したフィッシングやソーシャルエンジニアリングの手法・技術によるリスクが高まっているため、メール、チャットボット、AI 生成の音声/映像コンテンツを通じて従業員を標的とする新たな傾向を網羅した、最新の意識向上およびトレーニングを重視する。  <b>参考情報例：</b> ATLAS; ATT&CK; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>

<sup>1</sup> 2025 年 7 月に発表された米国の AI 行動計画には、米国国土安全保障省が主導し、米国商務省傘下の NIST 人工知能標準・イノベーションセンター（CAISI）および国家サイバー長官室と連携して、AI-ISAC の設立を進めるよう推奨する内容が含まれている <sup>7</sup> 例えば、OWASP は LLM と ML 向けの「トップ 10」リストを公開している。

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		<p>ーン; ENISA 脅威状況 2025; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>グ、ディープフェイク、エージェント操作など) を考慮に入れる。防御チームはこれらの脅威を識別・記録・分析するプロセスを確立すべきだ。</p> <p><b>参考情報例</b> : ENISA 脅威状況 2025 ; DASF 39 ; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ; AI 100-2e2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	
<p><b>ID.RA-04: 脆弱性を悪用する脅威の潜在的な影響と発生可能性を識別し記録する</b></p>	<p><b>一般的な考慮事項</b> : AI は全ての重点領域に新たな特有の考慮事項をもたらす。MITRE ATLAS™ などのリソースは組織が影響を理解するのに役立つ。</p> <p><b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : PM-09 ; PM-11 ; RA-02 ; RA-03 ; RA-08 ; RA-09</p>	<p><b>提案優先度</b> : 1</p> <p><b>重点領域の考慮事項例</b> : AI システムは、敵対的入力、データ漏洩、データ・ポイズニング、誤差増幅フィードバックループ、概念ドリフトなど、多くの新たな攻撃ベクトルをもたらす。</p> <p><b>参考情報例</b> : DASF 6, 13, 22-23, 45; OWASP AI Exchange: ガバナンス全般統制; OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025; <a href="https://arxiv.org/pdf/2504.11168">https://arxiv.org/pdf/2504.11168</a>; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度</b> : 1</p> <p><b>重点領域の考慮事項例</b> : AI を活用したサイバー防御の利用に伴い生じる新たなリスク要因 (例 : データ漏洩、過度の依存、過剰な自律性) をリスクモデリングに含めること。</p> <p><b>参考情報例</b> : DASF 38,39; OWASP AI Exchange: How about 生成的 AI?; ATLAS AML.M0005; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a>; AI 100-2e2025</p>	<p><b>提案優先度</b> : 1</p> <p><b>重点領域の考慮事項例</b> : AI を活用した攻撃は既存の脆弱性を標的とし、脆弱性の発見を支援する。リスク分析と脆弱性管理を優先すべきだ。<b>参考情報例</b> : NIST SP 800-218 (全編) ; ATLAS AML.M0016 ; ATT&amp;CK M1051 ; <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ; AI 100-2e2025</p>
<p><b>ID.RA-05: 脅威、脆弱性、発生確率、影響度を用いて固有リスクを理解し、リスク</b></p>	<p><b>一般的な考慮事項</b> : 脅威、発生可能性、影響に基づいて対策を優先順位付けし、高リスクな AI エラーを低減する。</p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : DASF 6, 13, 19, 36 ; OWASP AI Exchange : ガバナンス全般統</p>	<p><b>提案優先度</b> : 2</p> <p><b>機会例</b> : AI は複雑な技術データを明確なビジネス言語に変換する。具体的には技術的リスクを簡潔な洞察に要約し、経営陣が情報に基づいたリスク判断を下せるよう支援する。</p>	<p><b>提案優先度</b> : 2</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。(理由) リスク対応の優先順位付けにおいて、AI を活用した攻撃の影響を考慮に入れること。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
対応の優先順位付けに反映させる	参考情報例：NIST SP 800-53、改訂 5 版：PM-16；RA-02；RA-03；RA-07	制；OWASP LLM Top Ten：LLM03 サブライチェーン ENISA 脅威状況 2025； <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>重点領域の考慮事項例：</b> AI サイバーセキュリティ防御機能を継続的に評価し、展開前に十分な成熟度があることを確認する。 <sup>2</sup> <b>参考情報例：</b> DASF 38；ENISA 脅威状況 2025； <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ；AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>参考情報例：</b> <a href="https://arxiv.org/pdf/2309.01029">https://arxiv.org/pdf/2309.01029</a> ； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>
<b>ID.RA-06:</b> リスク対応策の選定、優先順位付け、計画策定、進捗管理、および情報共有	<b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。 <b>参考情報例：</b> NIST SP 800-53, Rev 5: PM-09; PM-18; PM-30; RA-07	<b>提案優先度：3</b> <b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。 <b>参考情報例：</b> DASF 12-13、36、38；OWASP AI Exchange：全般ガバナンス管理策；OWASP LLM トップ 10：LLM03 サブライチェーン；ENISA 脅威状況 2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>提案優先度：2</b> <b>機会例：</b> AI は積極的なリスクマネジメントやインシデント結果の予測に活用できる。これにより迅速な対応が可能となり、リスク対応策の立案やそれらの決定事項のコミュニケーション支援ができる。AI は脆弱性を分析して早期警告を発し、インシデント発生前に防御策の優先順位付けを支援する。 <b>重点領域の考慮事項例：</b> リスク対応時に AI 自律機能を無効化する条件を定義すると同時に、AI によるインシデント結果の予測を活用し、リスク対応の優先順位付けと伝達を行う。 <b>参考情報例：</b> DASF 38,39；ENISA 脅威状況 2025；AI 100-2e2025；	<b>提案優先度：1</b> <b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。（理由）組織が直面する基本的なリスクと脅威は、AI の存在によって増大する。また AI は、サイバー攻撃を実行する障壁を低下させる。ただし、このサブカテゴリに対して組織が実施すべきサイバーセキュリティ対策は変わらない。 <b>参考情報例：</b> <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>

<sup>2</sup> 技術準備度を示す一例として：<https://cloud.google.com/blog/products/identity-security/rsa-introducing-ai-powered-insights-threat-intelligence>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
			<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	
<b>ID.RA-07:</b> 変更と例外は管理され、リスク影響がアセスメントされ、記録され、追跡される	<p><b>一般的な考慮事項:</b> AI システムの変更が全体的な機能性を与える影響を予測するのは困難である。組織はバージョン管理プロセスを用いて、ハードウェア、ソフトウェア、設定値、またはトレーニングデータへの変更を記録すべきである。AI を利用するサイバーセキュリティ防御においては、モデル、トレーニングデータ、およびモデル設定 (例: ハイパーパラメータ) への変更を検証し記録すること。</p> <p><b>参考情報例:</b> NIST SP 800-53、改訂 5 版: CA-07; CM03; CM-04</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AI システムへのわずかな変更でさえ、事前に予測不可能なリスクをもたらす可能性がある。モデル変更の影響を予測することは、実際に変更を加え、結果として生じる AI をテストせずに困難 (あるいは不可能) である。</p> <p><b>参考情報例:</b> DASF 7、13-18、29、41、52; OWASP AI Exchange: ガバナンス全般統制; ENISA 脅威状況 2025</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。(理由) サイバーセキュリティ防御は組織保護において極めて重要な役割を果たす。</p> <p><b>参考情報例:</b> DASF 50; ENISA 脅威動向 2025; AI 100-2e2025</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。(理由) 変更は、たとえ軽微なものであっても、AI を活用した攻撃に悪用される可能性のあるシステムの脆弱性を生じさせる恐れがある。</p> <p><b>参考情報例:</b> NIST SP 800-172 - 構成管理 (3.4.1e-3.4.3e); NIST SP 800-172 - セキュリティアセスメント (3.12.1e); ATT&amp;CK M1033; ATT&amp;CK M1054</p>
<b>ID.RA-08:</b> 脆弱性開示の受領、分析、対応プロセスが確立されている	<p><b>一般的な考慮事項:</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例:</b> NIST SP 800-53、改訂 5 版: RA-05</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 12-13、19、53; OWASP AI Exchange: ガバナンス統制; OWASP LLM トップ 10: LLM03 サプライチェーン; ENISA 脅威状況 2025</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 38,50; ENISA 脅威状況 2025</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。(理由) AI を活用した攻撃は脆弱性を大規模に悪用する速度と効率性が高いため、脆弱性管理、開示、対応はより高い優先度が必要となる。</p> <p><b>参考情報例:</b> NIST SP 800-218 (全編); ATT&amp;CK M1016; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<b>ID.RA-09:</b> ハードウェアおよびソフトウェアの真正性と完全性は、取得および使用前に評価される	<p><b>一般的な考慮事項：</b>一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b>NIST SP 800-53、改訂 5 版：SA-04；SA05；SA-10；SA-11；SA-15；SA-17；SI-07；SR-05；SR-06；SR-10；SR-11</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。(理由) 真正性と完全性を検証する手法自体は変わらないが、サードパーティ製ツールの可視性が低い AI 環境では、その重要性が増す。</p> <p><b>参考情報例：</b>DASF 23、45、52；OWASP 従来型ランタイム制御；OWASP AI Exchange：全般ガバナンス制御；OWASP モデル入力機密性；OWASP LLM トップ 10：LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>DASF 50；OWASP AI Exchange：一般的なガバナンス制御；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。(理由) 承認されていない AI や悪意のある AI の使用を防ぐため、偽造ハードウェアやソフトウェアの使用を防止する追加対策が必要となる場合がある。</p> <p><b>参考情報例：</b>NIST SP 800-218 (全編)；ATT&amp;CK M1033；ATT&amp;CK M1054；ATT&amp;CK M1044；AI 100-2e2025</p>
<b>ID.RA-10:</b> 重要サプライヤーは調達前に評価される	<p><b>一般的な考慮事項：</b>一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b>NIST SP 800-53、改訂 5 版：SR-06</p>	<p><b>提案優先度：</b>3</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>DASF 7、12-14、19、29、35-39、41-42、46、51-53、55；OWASP AI Exchange：一般的なガバナンス管理；OWASP LLM トップ 10：LLM03 サプライチェーン</p>	<p><b>提案優先度：</b>3</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b>DASF 50；OWASP AI Exchange：一般的なガバナンス管理</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。(理由) 内部データ、システム、ソフトウェアへのアクセス権を持つサプライヤーやサードパーティは、AI を活用したサイバー攻撃の標的となる可能性がある。</p> <p><b>参考情報例：</b>NIST SP 800-218 (全編)；ATT&amp;CK M1047</p>
<b>改善点 (ID.IM)</b>	組織のサイバーセキュリティリスクマネジメントプロセス、手順、活動における改善は、すべての CSF 機能において識別される			
<b>ID.IM-01:</b> 評価から改善点が特定される	<p><b>一般的な考慮事項：</b>AI は検討すべき新たな指標群をもたらす。組織の目標と密接に連動する指標を慎重に選択せよ。例えば、偽陽性 (FP) が偽陰性 (FN) よりはるかに重要である場合、評価</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>機械学習における評価は慎重に検討すべきだ。評価データセットの構造や形式、データに存在する可能性のあるバイアスを考慮すること。また、モデルの性能</p>	<p><b>提案優先度：</b>3</p> <p><b>機会例：</b>AI は明確なインシデント概要やコンプライアンス報告書のドラフト、証拠の整理、標準文書の生成を通じて、アナリストの作業負担を軽減する。</p>	<p><b>提案優先度：</b>2</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。(理由) 組織は、AI を活用したサイバー攻撃のペースと規模に対応するため、AI 支援型防御の活用と導入</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	<p>指標は再現率 (recall) より精度 (precision) に大きく影響され、F1 スコアのような指標の使用は結果を曖昧にする可能性がある。</p> <p>フィードバックループを組み込み、サイバーセキュリティ活動における AI の活用を継続的に改善する。</p> <p><b>参考情報例：</b> NIST SP 800-53 第 5 版：AC-01；AT-01；AU-01；CA-01；CM-01；CP-01；IA-01；IR-01；MA-01；MP-01；PE-01；PL-01；PM-01；PS-01；PT-01；RA-01；SA-01；SC-01；SI-01；SR-01；CA-02；CA-05；CA-07；CA-08；CP-02；IR-04；IR-08；PL-02；RA-03；RA-05；RA-07；SA-08；SA-11；SA-17(06)；SI-02；SI04；SR-05</p>	<p>を測定する適切な指標を識別することも検討すべきだ。</p> <p>多くの場合、精度だけでは性能の適切性を完全に反映しない。</p> <p><b>参考情報例：</b> OWASP AI Exchange：望ましくない行動の影響を制限する制御；OWASP 従来型ランタイム制御；OWASP AI Exchange：一般的なガバナンス制御；OWASP AI Exchange：モデルアクセス制御；OWASP モデル入力制御；OWASP GenAI セキュリティプロジェクト：監視；OWASP LLM トップ 10：LLM03 サプライチェーン；ENISA 脅威状況 2025；AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>重点領域の考慮事項例：</b> AI モデルの性能指標 (精度/再現率、ドリフト率など) を、誤検知削減や敵対的堅牢性といったセキュリティ目標に対して評価し、継続的なセキュリティ改善点を識別する。</p> <p><b>参考情報例：</b> DASF 38,39,50；OWASP AI Exchange: Model Access Control；ATLAS AML.M0008；ENISA 脅威状況 2025；AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>を検討すべきである。指針については「防御」重点領域の機会と検討事項を参照のこと。</p> <p><b>参考情報例：</b> <a href="https://ieeexplore.ieee.org/document/10747338">https://ieeexplore.ieee.org/document/10747338</a>；AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<b>ID.IM-02:</b> セキュリティテストや演習から改善が識別される。これには、サプライヤーや関連するサードパーティと連携して実施されたものも含まれる	<p><b>一般的な考慮事項：</b> 改善点は、AI レッドチーム演習および AI モデルとデータのサプライヤーとの協調テストを通じて特定され、サプライチェーンを強化する。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AC-01；AT-</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 13；DASF 16；DASF 19；DASF 36；DASF 39；DASF 41；DASF 44；DASF 46；DASF 56；OWASP AI Exchange：望ましくない行動</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 39；OWASP AI Exchange：モデルアクセス管理；ATLAS AML.M0018；ENISA 脅威状況 2025；</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。(理由) 組織は、セキュリティテスト実施時に AI 支援型ペネトレーションテストおよびレッドチームツールを活用・導入し、AI を活用したサイバー攻撃のペースと規模に対応することを検討できる。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	01 ; AU-01 ; CA-01 ; CM-01 ; CP-01 ; IA-01 ; IR-01 ; MA-01 ; MP-01 ; PE01 ; PL-01 ; PM-01 ; PS-01 ; PT-01 ; RA-01 ; SA-01 ; SC-01 ; SI-01 ; SR-01 ; CA-02 ; CA-05 ; CA-07 ; CA-08 ; CP02 ; CP-04 ; IR-03 ; IR-04 ; IR-08 ; PL02 ; PM-04 ; PM-31 ; RA-03 ; RA-05 ; RA-07 ; SA-08 ; SA-11 ; SI-02 ; SI-04 ; SR-05	の影響を制限する制御 ; OWASP 従来型ランタイム制御 ; OWASP AI Exchange: 一般的なガバナンス制御 ; OWASP AI Exchange: モデルアクセス管理 ; OWASP モデル入力制御 ; OWASP GenAI セキュリティプロジェクト: 監視 ; OWASP LLM トップ 10: LLM03 サプライチェーン ; ENISA 脅威状況 2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	参考情報例 : NIST SP 800-172 – セキュリティアセスメント (3.12.1e) ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>
<b>ID.IM-03: 業務プロセス、手順、活動の実行から改善が識別される</b>	<p>一般的な考慮事項 : 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例 : NIST SP 800-53、改訂 5 版 : AC-01 ; AT-01 ; AU-01 ; CA-01 ; CM-01 ; CP-01 ; IA-01 ; IR-01 ; MA-01 ; MP-01 ; PE01 ; PL-01 ; PM-01 ; PS-01 ; PT-01 ; RA-01 ; SA-01 ; SC-01 ; SI-01 ; SR-01 ; CA-02 ; CA-05 ; CA-07 ; CA-08 ; CP-02 ; IR-04 ; IR-08 ; PL-02 ; PM-04 ; PM-31 ; RA-03 ; RA-05 ; RA-07 ; SA04 ; SA-08 ; SA-11 ; SI-02 ; SI-04</p>	<p>提案優先度 : 3</p> <p>重点領域の考慮事項例 : 標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例 : DASF 5 ; DASF 13 ; DASF 16 ; DASF 18 ; DASF 19 ; DASF 24 ; DASF 29 ; DASF 33 ; DASF 36 ; DASF 38 ; DASF 39 ; DASF 41 ; DASF 42 ; DASF 44 ; DASF 46 ; DASF 51 ; DASF 55 ; DASF 56 ; DASF 60 ; DASF 64 ; OWASP AI Exchange: 意図しない動作の影響を制限する制御 ; OWASP 従来型ランタイム制御 ; OWASP AI Exchange: 一般的なガバナンス制御 ; OWASP AI Exchange: モデルアクセス管理 ; OWASP モデル入力制御 ; OWASP GenAI セキュリティプロジェクト : 監視 ; OWASP LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025 ;</p>	<p>提案優先度 : 3</p> <p>重点領域の考慮事項例 : AI を活用した防御システムにおける継続的なセキュリティ改善を推進するため、高い人的介入率、頻繁なモデルドリフト警報、敵対的入力検知パターンなどの運用フィードバックを分析すべきである。</p> <p>参考情報例 : DASF 21,39 ; ATLAS AML.M0008 ; ATLAS AML.M0015 ; ENISA 脅威状況 2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>提案優先度 : 3</p> <p>重点領域の考慮事項例 : 標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例 : <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>		
<b>ID.IM-04:</b> 運用に影響を与えるインシデント対応計画およびその他のサイバーセキュリティ計画は、策定され、コミュニケーションされ、維持され、改善される	<p><b>一般的な考慮事項:</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例:</b> NIST SP 800-53、改訂 5 版: CP-02; IR-08; PL-02; SR-02</p>	<p><b>提案優先度:</b> 3</p> <p>AI システムに関連するインシデントには、特定の対応手順が存在する。これには以下が含まれるが、これらに限定されない: モデルのアクセス範囲 (データ、ツール、ネットワークなど) を縮小すること、ログを通じて問題を識別すること、安定したモデルのバックアップを復元すること (コードのバージョン管理だけでなく、モデルのバージョン管理、場合によっては過去のデータセットバージョンも利用する)。</p> <p><b>参考情報例:</b> DASF 19; DASF 39; DASF 41; OWASP AI Exchange: 全般ガバナンス管理策; OWASP LLM トップ 10: LLM03 サプライチェーン; ENISA 脅威状況 2025; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> インシデント対応計画には、封じ込め (例: モデルの自律性を無効化)、トリアージ (例: モデルログの分析)、復旧 (例: 妥当性確認モデルバージョンの復元) といった AI 固有の手順を含める。</p> <p><b>参考情報例:</b> DASF 39; ENISA 脅威状況 2025; ATLAS AML.M0014; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案された優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。(理由) これらの計画の改善は、AI を活用した攻撃の進化と、(あらゆる) 効果的な緩和や実施された対策を反映する必要がある。これにより、PR.AT-01、特に PR.AT-02 に関連する取り組み、および継続的な監視と異常活動の検知が改善される可能性がある AI を活用した攻撃の実行速度、高度化や欺瞞の速度を考慮すると、ここでの更新はより動的である可能性が高い。</p> <p><b>参考情報例:</b> NIST SP 800-172 – インシデント対応 (3.6.1e-3.6.2e); AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<b>防御 (PR)</b>	組織のサイバーセキュリティリスクを管理するための安全対策が用いられる			
<b>識別管理、認証、アクセス管理 (PR.AA)</b>	物理的および論理的資産へのアクセスは、認可されたユーザー、サービス、ハードウェアに限定され、不正アクセスの評価リスクに見合った方法で管理される			
<b>PR.AA-01:</b> 認可されたユーザー、サービス、ハードウェアの識別情報と認証情報は組織によって管理される	<p><b>一般的な考慮事項:</b> AI システムに固有で追跡可能な識別子と認証情報を付与し、その活動をより適切に追跡できるようにする。</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> AI システムは、より広範なシステムと相互作用するために、独自の識別子と認証情報 (すなわち AI サービスレベルアカウント) を必要とする可能性がある。組</p>	<p><b>提案優先度:</b> 2</p> <p><b>機会例:</b> AI は、異常な認証活動をフラグ付けすることで、従来のルールでは見逃す可能性のある認証情報の不正使用を検知する。</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。(理由) AI を活用したサイバー攻撃は、ID や認証情報、サービス、ハードウェアへのアクセス障壁を低下さ</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	<p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AC-01；AC-02；AC-14；IA-01；IA-02；IA-03；IA-04；IA-05；IA-06；IA-07；IA-08；IA-09；IA-10；IA-11</p>	<p>織は、AI システムとその動作の間の追跡可能性を必要とする。</p> <p><b>参考情報例：</b> DASF 1、3、21-22、32、40、48；ATLAS AML.M0005；ATLAS AML.M0019；OWASP AI Exchange：意図しない動作の影響を制限する制御；OWASP 従来型ランタイム制御；OWASP AI Exchange：モデルアクセス管理；OWASP LLM トップ 10: LLM03 サプライチェーン；ENISA 脅威状況 2025；AI 100-2e2025</p>	<p><b>重点領域の考慮事項例：</b> 防御対応活動を支援するため、AI 防御エージェントに一意で追跡可能な識別子と認証情報を割り当て、管理する。</p> <p><b>参考情報例：</b> DASF 39；WASP AI Exchange：モデルアクセス管理；ENISA 脅威状況 2025；ATLAS AML.M0005</p>	<p>せる。<b>参考情報例：</b> NIST SP 800-172 – 構成管理 (3.4)；NIST SP 800-172 <b>識別と認証 (3.5)</b>；NIST SP 800-207 – ゼロトラストアーキテクチャ；ATT&amp;CK M1032</p> <p>管理 (3.4)；NIST SP 800-172 識別と認証 (3.5)；NIST SP 800-207 – ゼロトラストアーキテクチャ；ATT&amp;CK M1032；ATT&amp;CK M1027；ATLAS AML.M0005；ATLAS AML.M0019；AI 100-2e2025</p>
<b>PR.AA-02:</b> 相互作用の文脈に基づき、身元は検証され、認証情報に紐付けられる	<p><b>一般的な考慮事項：</b> LLM や AI エージェントは、通常ユーザーがアクセスできないデータソースやツールを利用できる場合がある。暗号署名と相互認証を用いて、エージェントとサービスの身元をその認証情報に紐付けること。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：IA-12</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 1、3-5、22、32-33、40、57；<a href="#">ATLAS AML.M0005</a>；<a href="#">ATLAS AML.M0026</a>；<a href="#">ATLAS AML.M0027</a>；<a href="#">ATLAS AML.M0028</a>；OWASP 従来型ランタイム制御；AI 100-2e2025</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> AI サービスは過剰な自律性を防ぐため、文脈と時間に縛られるべきだ。証明書ベースの妥当性確認を義務付け、エージェントの動作を継続的に監視することでありすましを防止し、悪意のあるツールが組織の防御エージェントを模倣できないようにする。</p> <p><b>参考情報例：</b> DASF 39,50；ENISA 脅威状況 2025；ATLAS AML.M0013；AML.M0014)；AI 100-2e2025</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。(理由) AI を活用したサイバー攻撃は、ID や認証情報、サービス、ハードウェアへのアクセス障壁を低下させる。</p> <p><b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。</p>
<b>PR.AA-03:</b> ユーザー、サービス、ハードウェアは認証される	<p><b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AC-07；AC12；IA-02；IA-03；IA-</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 1-2、4-5、18、21-22、24、29、31-33、40、42-43、46、56、64；ATLAS AML.M0005；OWASP</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 各 AI エージェントに固有の ID と認証情報を割り当て、特権ユーザーと同等のセキュリティ対策を適用する。</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。(理由) AI を活用したサイバー攻撃は、ID や認証情報、サービス、ハードウェアへのアクセス障壁を低下させるが、これらの攻撃を緩和する方法は変わらない。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	05 ; IA-07 ; IA-08 ; IA-09 ; IA-10 ; IA-11	従来型ランタイム制御 ; ENISA 脅威状況 2025	<b>参考情報例</b> : DASF 39,50 ; ENISA 脅威動向 2025 ; ATLAS AML.M0019 ; ATLAS AML.M0005 ; AI 100-2e2025	<b>参考情報例</b> : AI 固有の参考情報例は追加情報待ち。
<b>PR.AA-04:</b> 身元主張は防御され、伝達され、検証される	<p><b>一般的な考慮事項</b> : 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : IA-13</p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : DASF 22、40</p>	<p><b>提案優先度</b> : 2</p> <p><b>重点領域の考慮事項例</b> : アイデンティティアサーションは、AI コンポーネントが有効であるという保証を提供する。エージェント主張とトークンの署名および検証は、それらの来歴証明に関する知見を提供し、組織が期待されるエージェントのみが動作していることを確認することを支援する。</p> <p><b>参考情報例</b> : DASF 39 ; OWASP AI Exchange : 利用監視 ; ATLAS AML.M0013 ; ATLAS AML.M0014 ; AI 100-2e2025</p>	<p><b>提案優先度</b> : 2</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。(理由) AI を活用したサイバー攻撃は、ID や認証情報、サービス、ハードウェアへのアクセス障壁を低下させるが、これらの攻撃を緩和する方法は変わらない。</p> <p><b>参考情報例</b> : AI 固有の参考情報例は追加情報待ち。</p>
<b>PR.AA-05:</b> アクセス権限、の権限付与、および認可はポリシーで定義され、管理、適用、およびレビューされ、最小権限の原則と職務分離の原則を取り入れる	<p><b>一般的な考慮事項</b> : AI システムはネットワーク内の他の事業体とは別個に扱い、独自の権限と認可ポリシーを必要とする。最小権限の原則を適用し、AI エージェントにはその役割を遂行するために必要な権限のみを付与する。</p> <p><b>参考情報例</b> : NIST SP 800-53, Rev 5: AC-01; AC-02; AC-03; AC-05; AC-06; AC-10; AC-16; AC-17; AC-18; AC-19; AC24; IA-13</p>	<p><b>提案優先度</b> : 1</p> <p><b>重点領域の考慮事項例</b> : AI システムは複雑かつ予測不可能な方法で相互作用する可能性があるため ( )、その権限と認可を管理する新たな方針セットが必要となるかもしれない。</p> <p><b>参考情報例</b> : DASF 2-3、5-6、14、18、21、22、24、29、31-33、40、42-43、46、51、5658、60、64 ; ATLAS AML.M0005 ; ATLAS AML.M0012 ; ATLAS <a href="#">AML.M0026</a> ; <a href="#">ATLAS AML.M0027</a> ; OWASP AI Exchange: 意図しない動作の影響を制限する制御; OWASP 従来型ランタイム制御; OWASP</p>	<p><b>提案優先度</b> : 2</p> <p><b>機会例</b> : AI は、異常な認証活動をフラグ付けすることで、従来のルールでは見逃される可能性のある認証情報の不正使用を検知する。</p> <p><b>重点領域の考慮事項例</b> : AI エージェントの権限を時間軸で管理するプロセスを確立する (例 : 定期的なレビューと更新) は、他の特権アカウンと同様に扱われる。</p> <p><b>参考情報例</b> : OWASP AI Exchange : 最小限のモデル権限 ; DASF 39,50 ; ENISA 脅威状況 2025 ; ATLAS AML.M0005 ; ATLAS AML.M0019 ; ATLAS AML.M0026 ; ATLAS AML.M0027 ;</p>	<p><b>提案優先度</b> : 1</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。(理由) スケーラブルなブルートフォース攻撃などの手法で認証情報やアクセスキー/トークンなどを取得しようとする AI を活用したサイバー攻撃を防ぐため、アクセス管理と認可に関する堅牢なポリシーを維持する。</p> <p><b>参考情報例</b> : AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917">https://arxiv.org/html/2503.11917</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		AI Exchange: モデルアクセス管理; OWASP LLM トップ 10: LLM03 サプライチ ーン; ENISA 脅威状況 2025_ <a href="https://arxiv.org/pdf/2504.11168">https://arxiv.org/pdf/2504.11168</a> ; AI 100-2e2025;_ <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	ATLAS AML-M0028 ; AI 100-2e2025;_ <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	
<b>PR.AA-06:</b> 資産への物理的アクセスは、リスクに見合った方法で管理、監視、および実施される	<p><b>一般的な考慮事項:</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例:</b> NIST SP 800-53、改訂 5 版: PE-02 ; PE-03 ; PE-04 ; PE-05 ; PE-06 ; PE-08 ; PE-18 ; PE-19 ; PE-20</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 1、4-5、9、16、21-22、24、31、40、46、56、57、59、62 ; ATLAS AML.M0005 ; ATLAS AML.M0012</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AI 搭載システムを活用して物理的防御能力を強化する。例えば、コンピュータービジョンを用いてデータセンターやグラフィックス処理装置 (GPU) ラックにおける不正アクセス、改ざん、侵入を検知する。</p> <p><b>参考情報例:</b> ENISA 脅威動向 2025 ; DASF 39 ; ATLAS AML.M0005 ; ATLAS AML.M0009 ; AI 100-2e2025</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> AI 固有の参考情報例は追加情報待ち。</p>
<b>意識向上およびトレーニング (PR.AT)</b>	組織の職員には、サイバーセキュリティ関連の業務を遂行できるよう、サイバーセキュリティに関する意識向上およびトレーニングがプロバイダによって提供される			
<b>PR.AT-01:</b> 職員は、一般的なサイバーセキュリティリスクに関連する業務を遂行するための知識と技能を身につけるよう、プロバイダにより意識向上およびトレーニングが提供される。	<p><b>一般的な考慮事項:</b> AI システムの結果を扱うには、十分な訓練が必要だ。AI システムは急速に進化し、予測不能な出力を生むことがあるからだ。</p> <p>この研修は、AI 技術の発展のペースに合わせるため、頻繁に更新し、再実施する必要がある。</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> AI はサイバーセキュリティの領域に、これまでに見られなかった新たな次元をもたらす。担当者は、モデルの限界、敵対的入力、概念ドリフトといった新たな考慮事項、およびこれらが特定の状況にどう適用されるかを認識すべきだ。</p> <p><b>参考情報例:</b> DASF 25, 32, 39, 41, 61; ATLAS AML.M0012; ENISA 脅威状況</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> AI の使用は、幻覚や虚構といった情報の正確性に対するリスクをもたらす。行動前に幻覚、バイアス、操作された応答、その他の潜在的問題を検知するため、エージェントの監視方法と AI 出力の評価方法を分ける者に訓練させること。</p> <p><b>参考情報例:</b> DASF 25,31,32,29,41,6;_ <a href="https://arxiv.org/pdf/2311.05232">https://arxiv.org/pdf/2311.05232</a>;</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> AI はサイバーセキュリティ脅威の領域に、これまでに見られなかった新たな次元をもたらす。担当者は、スピアフィッシングやソーシャルエンジニアリングの手法を利用するといった、AI を活用した新たな脅威について認識し、関連する研修を受ける機会を持つべきだ。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
サイバーセキュリティリスクを伴う	<b>参考情報例</b> : NIST SP 800-53 第 5 版 : AT-02 ; AT-03	2025; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	ENISA 脅威状況 202; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>参考情報例</b> : NIST SP 800-172 – 意識向上およびトレーニング (3.2); ATT&CK M1017; ATLAS AML.M0018; NIST AI 600-1 MP-5.1-002; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>
<b>PR.AT-02:</b> 専門的な役割を担う個人には、関連する業務を遂行するための知識と技能を身につけさせるため、意識向上およびトレーニングがプロバイダによって提供される。 サイバーセキュリティリスクを 考慮事項 : AI システムの使用または AI を活用した攻撃からの防御を担当する専門職は、サイバーセキュリティと	<b>一般的な考慮事項</b> : AI システムの使用または AI を利用した攻撃からの防御を担当する専門的役割は、サイバーセキュリティと AI 固有の脅威、および関連する緩和戦略の両方を認識している。 <b>参考情報例</b> : NIST SP 800-53, Rev 5: AT-03	<b>提案優先度</b> : 2 <b>重点領域の考慮事項例</b> : AI はサイバーセキュリティの領域に新たな次元をもたらす。AI システムの防御を担当する者は、組織の状況に適用可能なサイバーセキュリティ全般の考慮事項 ( ) と AI 固有の考慮事項の両方を認識すべきである。 <b>参考情報例</b> : DASF 25, 39, 61; ATLAS AML.M0012; ENISA 脅威状況 2025; AI 100-2e2025	<b>提案優先度</b> : 1 <b>機会例</b> : AI は防御体制をテストし、防御担当者が対応スキルを練習・向上させるための現実的な攻撃シミュレーションやフィッシングシナリオを生成する。 <b>重点領域の考慮事項例</b> : レッドチーム活動と要員訓練では、AI を活用した防御行動、敵対的機械学習、プロンプト・インジェクション、モデルドリフト、AI フォレンジックに対応すべきだ。これにより要員は、組織のニーズとリスク許容度に合致した AI 防御行動を活用する技能と知識を構築できる。 <b>参考情報例</b> : DASF 25,32,39,41,61; ATLAS AML.M0018; AML.M0003; AI 1002e2025	<b>提案優先度</b> : 1 <b>重点領域の考慮事項例</b> : AI はサイバーセキュリティ脅威の新たな次元をもたらす。職員は、標的型フィッシングやソーシャルエンジニアリングの手法を利用するような、AI を活用した新たな脅威に関する訓練と情報にアクセスできる必要がある。AI を活用したフィッシング、ソーシャルエンジニアリング、チャットボットの活用に関する最新の訓練は、サイバーセキュリティインシデントを阻止するために不可欠である専門的な役割 (例 : インシデント対応) を担う要員は、AI を活用した攻撃を認識し、妥当性確認するための追加トレーニングが必要となる。効果的な検知、対応、復旧活動を促進するため、モデリングやシミュレーションシナリオの開発も必要となる可能性がある。 <b>参考情報例</b> : NIST SP 800-172 – 意識向上およびトレーニング (3.2) ; ATT&CK M1017 ; ATLAS AML.M0018 ; NIST AI 600-1 MP-5.1-002 ; AI 100-2e2025

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
データセキュリティ (PR.DS)	データは、情報の機密性、完全性、可用性を防御するため、組織のリスク戦略に沿って管理される			
PR.DS-01: 保管中のデータの機密性、完全性、可用性は防御される	<p><b>一般的な考慮事項：</b>データは多くの AI システムの機能にとって極めて重要である。AI 特有の機密性、完全性、可用性に関する懸念事項の例としては、可用性ポイズニングと可用性障害、完全性ポイズニング、機密性漏洩と侵害（プライバシー問題も引き起こし得る）が挙げられる。データが のように破損した場合、機械学習モデルはそのデータを用いて学習しなくなる。</p> <p>データが改ざんされると、モデルはうまく学習しない。こうした考慮事項は AI にとって極めて重要だが、組織がそれらを防ぐために用いる緩和は、他の種類のソフトウェア暗号化やデータバックアップと変わらない。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：CA-03；CP-09；MP-08；SC-04；SC-07；SC-12；SC-13；SC-28；SC-32；SC-39；SC-43；SI-03；SI-04；SI-07</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。（根拠）一般事項を参照のこと。</p> <p><b>参考情報例：</b> DASF 3-13、16-17、20-22、24-27、29-31、33、36、42、44、46、51、56、58-60、62；ATLAS AML.M0005；ATLAS AML.M0012；ATLAS AML.M0024；ATLAS AML.M0025；OWASP 従来型ランタイム制御；OWASP AI Exchange: 一般 ガバナンス；OWASP モデル入力機密性；OWASP GenAI セキュリティプロジェクト: 監視；OWASP LLM トップ 10: LLM03 サプライチェーン；ENISA 脅威状況 2025；AI 100-2e2025</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> 正確で大規模かつ迅速な防御活動を可能にするには、信頼できるデータが必要だ。</p> <p><b>参考情報例：</b> DASF 32,39,41；ENISA 脅威状況 2025 ATLAS AML.M0012；ATLAS AML.M0005；AI 100-2e2025</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。（根拠）一般事項を参照のこと。</p> <p><b>参考情報例：</b> ATT&amp;CK M1057；ATT&amp;CK M1053；ATT&amp;CK M1041；ATT&amp;CK M1029；ATLAS AML.M0007；AI 100-2e2025</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
PR.DS-02: 転送中のデータの機密性、完全性、可用性が防御されている	<p><b>一般的な考慮事項:</b> AI 特有の機密性、完全性、可用性に関する懸念事項の例には、可用性ポイズニングと可用性障害、完全性ポイズニング、機密性漏洩と侵害（プライバシー問題も引き起こし得る）が含まれる。</p> <p><b>参考情報例:</b> NIST SP 800-53、改訂 5 版: AU-16; CA03; SC-04; SC-07; SC-08; SC-11; SC-12; SC-13; SC-16; SC-40; SC-43; SI03; SI-04; SI-07</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 3-5、7、9、11、13、16、21-27、29-34、36、44-46、51、56、58-60、62; ATLAS AML.M0024; OWASP 従来型ランタイム制御; OWASP AI Exchange: 一般的なガバナンス制御; OWASP モデル入力機密性; OWASP GenAI セキュリティプロジェクト: 監視; OWASP LLM トップ 10: LLM03 サプライチェーン; ENISA 脅威状況 2025</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 25,37,39; ENISA 脅威状況 2025; ATLAS AML.M0019</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 9; ATT&amp;CK M1057;</p>
PR.DS-10: 使用中のデータの機密性、完全性、可用性が防御される	<p><b>一般的な考慮事項:</b> AI は機密データにアクセスできる場合、常にその漏洩リスクを内在している。AI 特有の機密性、完全性、可用性に関する懸念事項の例としては、可用性ポイズニングと可用性障害、完全性ポイズニング、機密性漏洩と侵害（プライバシー問題も引き起こし得る）が挙げられる。一般的に、AI モデルは学習に使用されたデータおよび推論時にアクセス可能なデータと同等の機密性を有する。</p> <p><b>参考情報例:</b> NIST SP 800-53 第 5 版: AC-02; AC-</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> AI が利用しユーザーと共有する情報は、常に厳密に制御できるに限らない。二つのデータベースに接続された情報検索サービスを例に挙げよう。一つは構造化問い合わせ言語 (SQL) サーバーに接続されている。もう一つは AI を用いて意味的に情報を検索する検索サービスでは、取得・共有される情報を厳密に制御できる。一方、意味論的システムでは、クエリが意味論に基づいているため、共有されるデータを制御するのはより困難である。</p> <p><b>参考情報例:</b> DASF 5, 9, 11, 13, 15-16, 20-27, 29-34, 36, 42, 44-46, 56, 58-60, 62; ATLAS AML.M0024;</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> AI プロンプトや機能における機密データの使用を最小限に抑え、実行時編集とガードレールの使用を実施する。出力フィルタリング、パターン検知、アクセス管理を実施することでデータ漏洩を防止する。</p> <p><b>参考情報例:</b> DASF 25,34,40; ENISA 脅威状況 2025; <a href="https://arxiv.org/pdf/2303.00654">https://arxiv.org/pdf/2303.00654</a>; AI 100-2e2025</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> AI 固有の参考情報例は追加情報待ち。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	03 ; AC-04 ; AU-09 ; AU-13 ; CA-03 ; CP-09 ; SA-08 ; SC-04 ; SC-07 ; SC-11 ; SC-13 ; SC-24 ; SC-32 ; SC-39 ; SC-40 ; SC-43 ; SI-03 ; SI-04 ; SI-07 ; SI-10 ; SI16	OWASP (全項目) ; ENISA 脅威状況 2025; <a href="https://arxiv.org/pdf/2303.00654">https://arxiv.org/pdf/2303.00654</a> ; AI 100-2e2025		
<b>PR.DS-11:</b> データのバックアップを作成、防御、維持、テストする	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版：CP-06 ; CP-09</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：重要な AI 資産（妥当性確認されたモデルバージョン、クリーンなトレーニングデータセット、設定ファイルを含む）の保護されたバックアップを定期的にテストし、データ・ポイズニングやモデル侵害からの迅速な復旧を確保する。</p> <p>参考情報例：DASF 8, 15, 17, 20-22, 27-30, 41-42; ATLAS AML.M0012; ATLAS AML.M0024; ATLAS AML.M0025</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：妥当性確認されたモデルバージョン、クリーンなトレーニングデータセット、設定ファイルを含む重要な AI 資産の保護されたバックアップを定期的にテストし、データ・ポイズニングやモデル侵害からの迅速な復旧を確保する。</p> <p>参考情報例：ENISA 脅威状況 2025; DASF 17,38,50; ATLAS AML.M0014; ATLAS AML.M0007</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：NIST SP 800-53, Rev 5: CP-06, CP09;</p>
<b>プラットフォームセキュリティ (PR.PS)</b>	物理的および仮想的なプラットフォームのハードウェア、ソフトウェア（例：ファームウェア、オペレーティングシステム、アプリケーション）、サービスは、組織のリスク戦略に沿って管理され、これらの機密性、完全性、可用性を防御する			
<b>PR.PS-01:</b> 構成管理の実践が確立され、適用される	<p>一般的な考慮事項：AI システムのハイパーパラメータ設定は、システムの機能に極めて重要である。これらの設定値は、ソフトウェア本体と同等の厳格さで追跡、バージョン管理、管理される。</p> <p>参考情報例：NIST SP 800-53, Rev 5: CM-01; CM-02; CM-03; CM-04; CM-05;</p>	<p>提案優先度：1</p> <p>重点領域の考慮事項例：AI の性能は設定と密接に関連している。AI をより広範なシステムに追加する際、これらの追加設定も追跡・管理される。</p> <p>参考情報例：DASF 3, 5-8, 10, 18-19, 21, 23-24, 28-29, 31-33, 35, 41-46, 51-53, 58, 60, 63, 64; ATLAS</p>	<p>提案優先度：1</p> <p>重点領域の考慮事項例：AI モデル構成管理の実践を確立し適用する。具体的には、モデル構成、プロンプト、閾値、ガードレールルールのバージョン管理と追跡などである。</p> <p>参考情報例：DASF 38,40,41; ATLAS AML.M0023; ATLAS AML.M0021</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ慣行が適用される。</p> <p>参考情報例：NIST SP 800-218（全編）</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	CM-06; CM-07; CM-08; CM-09; CM-10; CM-11	AML.M0005; ATLAS AML.M0012; OWASP Conventional Runtime Controls; ENISA 脅威状況 2025		
<b>PR.PS-02:</b> ソフトウェアはリスクに見合った方法で保守、置換、削除される	<p><b>一般的な考慮事項:</b> AI 枠組みやソフトウェアライブラリに対して、定期的にパッチを確認し適用する。これは組織を守るためであり、攻撃が発生する前に防ぐためでもある。</p> <p><b>参考情報例:</b> NIST SP 800-53 第 5 版: CM-11; MA-03(06); SA-10(01); SI-02; SI-07</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 13、21、23、32、38、45、53、63; ENISA 脅威状況 2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> AI フレームワークやライブラリに対して定期的にパッチを確認し適用し、攻撃時に悪用される可能性のある脆弱性を塞ぐこと。</p> <p><b>参考情報例:</b> DASF 32,37,41; ENISA 脅威状況 2025</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 安全性が確保されておらず、テストもされておらず、あるいはメンテナンスされていないコードは、AI を活用したサイバー攻撃の標的となる可能性がある。リスク閾値を維持するため、脆弱性管理に基づき追加のコードスキャンと置換を実施する。ソフトウェアのライフサイクル全体を通じた維持管理手順に従うこと。</p> <p><b>参考情報例:</b> NIST SP 800-218 (全版); NTIA SBOM (全版); AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<b>PR.PS-03:</b> ハードウェアは、リスクに見合った方法で保守、交換、廃棄される。  リスクに見合った方法で	<p><b>一般的な考慮事項:</b> AI は新たなハードウェアセット（高速化コンピューティング）の需要を生み出す。この新規ハードウェアが定期的にテスト、保守、更新され、攻撃によるエクスポージャーを最小限に抑えることを保証する。</p> <p><b>参考情報例:</b> NIST SP 800-53, Rev 5: CM-07 (09)、SA-10(03)、SC-03(01)、SC-39(01)、SC-49、SC-51</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 6、10、18-19、29、42、59、63; OWASP 標準的な実行時制御; ENISA 脅威状況 2025</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> ハードウェアアクセラレータのファームウェアとドライバを頻繁に更新する。</p> <p><b>参考情報例:</b> DASF 38-39; ENISA 脅威状況 2025; ATLAS AML.M0016; AML.M0011</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> セキュリティ対策が不十分、テスト未実施、および/または保守されていないサイバーフィジカルハードウェアやシステムは、AI を活用した攻撃の標的となり得る。リスク閾値を維持するため、追加のハードウェアスキャンと交換が実施される。</p> <p><b>参考情報例:</b> ATT&amp;CK M1034</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
PR.PS-04: ログ記録が生成され、の継続的監視に利用可能となる	<p><b>一般的な考慮事項:</b> AI は、すべての重点領域に新たな固有の考慮事項をもたらす。</p> <p><b>参考情報例:</b> NIST SP 800-53, Rev 5 : AU-02, AU-03, AU-06, AU-07, AU-11, AU-12</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> AI はシステム全体を把握するために に記録すべき新たな指標とパラメータ群をもたらす。例えば検知閾値やその他の推論時間パラメータなどだ。</p> <p><b>参考情報例:</b> DASF 11-12, 14, 20-21, 23, 29, 32-33, 35-37, 39-40, 42, 44-46, 55, 60; ATLAS AML.M0005; OWASP 従来型ランタイム制御; OWASP GenAI セキュリティプロジェクト: 監視; ENISA 脅威状況 2025; AI 100-2e2025</p>	<p><b>提案優先度:</b> 1</p> <p><b>機会例:</b> AI を活用してログを分析・スキャンし、異常事象を自動検出する。AI を用いて 複数の情報源から情報を統合する。ログにはリクエストデータ、レスポンスデータ、およびレスポンスがポリシーに適合したか否かを記録すべきだ。</p> <p><b>重点領域の考慮事項例:</b> HITL レビューで発見内容を確認する。ログの防御を検討する。</p> <p><b>参考情報例:</b> DASF 32,39,41; ENISA 脅威状況 2025; AI 100-2e2025</p>	<p><b>提案優先度:</b> 1</p> <p><b>サンプルの重点領域に関する考察:</b> AI を活用した攻撃が のサイバーセキュリティ検知・監視システムに課題をもたらす一例が、その規模と速度である。検知と防御のためには、AI を活用した戦術・技術の新たなパターンを特定する継続的な監視と記録が必要となる。</p> <p><b>参考情報例:</b> AI 100-2e2025</p>
PR.PS-05: 許可されていないソフトウェアのインストールと実行は防止される	<p><b>一般的な考慮事項:</b> いかなるシステムからのコードの自動ダウンロードや実行も許可してはならない。全てのソフトウェアがマルウェアスキャンを受けており、ソフトウェアのソースが適切に審査されていることを確認すること。</p> <p><b>参考情報例:</b> NIST SP 800-53, 改訂 5 版 : CM-07(02), CM-07(04), CM-07(05), SC-34</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AI エージェントシステムは、任意のコードを実行することが許される場合がある。ほとんどのアプリケーションでは、この能力は制限され、サンドボックス化され、承認と監視の対象となるか、完全に禁止されるべきである。</p> <p><b>参考情報例:</b> DASF 7, 10-11, 13, 18-19, 29, 36, 44, 52, 54, 60; OWASP 標準ランタイム制御; OWASP GenAI セキュリティプロジェクト: 監視; OWASP LLM トップ 10 : LLM03 サプライチェーン</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> 承認されていないモデルのダウンロードや有用なエージェントスクリプトをブロックし、審査済みかつ認可されたコンポーネントのみが AI 防御環境に統合されるようにする。</p> <p><b>参考情報例:</b> DASF 1, 40; ATLAS AML.M0011; ATLAS AML.M0013</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 認可されていないコードやスキャンされていないコードは、悪意のある AI 対応パッケージやマルウェアがシステムに侵入する経路の一つだ。システム上の他の資産にアクセス可能な本番環境システムへのソフトウェアのダウンロードやインストールについては、厳格なガイドラインを維持すること。</p> <p><b>参考情報例:</b> AI 固有の参考情報例は追加情報待ち。</p>
PR.PS-06: セキュアなソフトウェア開発手法が統合され、その実施状況がソフトウェア	<p><b>一般的な考慮事項:</b> AI は通常のソフトウェア開発を超えた新たなセキュリティ指標群を導入する。これらの指標は考慮され、組織が</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AI は再現性、潜在能力、特定の入力に対するバイアス、不確</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> プロンプトテスト、敵対的テスト、評価ゲートを導入し、AI チェックを</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
開発ライフサイクル全体を通じて監視される	<p>追跡しているその他のセキュリティ指標に追加される。</p> <p><b>参考情報例：</b> NIST SP 800-53 第 5 版：SA-03；SA-08；SA-10；SA-11；SA-15；SA-15(13)；SA-17；SA-24</p>	<p>実なモデル出力に直面した際の対応策といった新たな性能上の考慮事項をもたらす。</p> <p><b>参考情報例：</b> NIST SP 800-218A；DASF 11, 19-20, 23, 41, 45, 52, 59；OWASP 従来型ランタイム制御；OWASP AI Exchange：全般ガバナンス制御；OWASP Model Input Confidentiality；OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025； <a href="https://arxiv.org/pdf/2504.11168">https://arxiv.org/pdf/2504.11168</a>；AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>ソフトウェア開発慣行の安全確保に拡大する。パフォーマンス監視中に安全性や品質が低下した場合、展開を阻止する。AI 搭載脆弱性スキャンツールから得た知見を適用し、AI システムの安全確保と AI 攻撃の阻止を図る。</p> <p><b>参考情報例：</b> DASF 38,41,45；ENISA 脅威状況 2025；ATLAS AML.M0008；ATLAS AML.M0003；AI 100-2e2025</p>	<p><b>参考情報例：</b> <a href="https://arxiv.org/pdf/2504.11168">https://arxiv.org/pdf/2504.11168</a></p>
<b>技術インフラのレジリエンス (PR.IR)</b>	セキュリティアーキテクチャは、組織のリスク戦略に基づいて管理され、資産の機密性、完全性、可用性、および組織のレジリエンスを防御する			
<b>PR.IR-01:</b> ネットワークと環境は、不正な論理的アクセスと使用から防御されている	<p><b>一般的な考慮事項：</b> AI がネットワーク内の新たなネットワークやシステムにアクセスする能力は、AI システムの機能性と組織が許容するリスクのレベルに応じて制限すべきである。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AC-03；AC04；SC-04；SC-05；SC-07</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> AI エージェントは、これまでに見られたエージェント（人間や従来型の制御ボット）とは異なる方法でネットワークや環境にアクセスしようとする可能性がある。AI エージェントのネットワーク・環境へのアクセスは、最小権限の原則に基づき、組織のリスク戦略に従って制限すべきである。</p> <p><b>参考情報例：</b> DASF 1-5, 7, 9-11, 16, 18-19, 21, 23-24, 28-34, 41, 43, 45-46, 52, 56-59, 64；ATLAS AML.M0005；ATLAS AML.M0012；</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の検討例：</b> 人間の承認またはポリシーに基づくチェックを実装し、AI が開始するネットワーク変更と特権使用を規制する。</p> <p><b>参考情報例：</b> DASF 38,40；ENISA 脅威状況 2025；ATLAS AML.M0019；AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> AI を活用した攻撃は、ネットワークへのアクセスや不正アクセス・不正利用の参入障壁を低下させる。防御策としては、エンドポイント検知システムや認証・ID 管理（MFA やゼロトラストアーキテクチャなど）に対する追加のセキュリティ層を優先すべきだ。</p> <p><b>参考情報例：</b> AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		OWASP AI Exchange: Controls to Limit the Effects of Unwanted Behavior; OWASP Conventional Runtime Controls; OWASP AI Exchange: モデルアクセス管理; OWASP AI Exchange: Rate Limit; OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025; <a href="https://arxiv.org/pdf/2504.11168">https://arxiv.org/pdf/2504.11168</a> ; AI 100-2e2025;_ <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>		
<b>PR.IR-02:</b> 組織の技術資産は環境的脅威から防御されている	<p><b>一般的な考慮事項:</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例:</b> NIST SP 800-53、改訂 5 版: CP-02; PE09; PE-10; PE-11; PE-12; PE-13; PE-14; PE-15; PE-18; PE-23</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> DASF 23、45</p>	<p><b>提案優先度:</b> 3</p> <p><b>重点領域の考慮事項例:</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例:</b> ENISA 脅威状況 2025; DASF 17、41; ATLAS AML.M0009; ATLAS AML.M0005</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AI を活用した攻撃は物理的資産 (例: 運用技術) に影響を与える可能性がある。</p> <p><b>参考情報例:</b> AI 100-2e2025</p>
<b>PR.IR-03:</b> 通常時および異常時におけるレジリエンス要件を達成するためのメカニズムが実装されている	<p><b>一般的な考慮事項:</b> AI モデルのレジリエンスを高める様々なシステムが存在する。これにはバックアップ、モデルの強化、アンサンブル手法、自動フェイルオーバーなどが含まれるが、これらに限定されない。</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AI の故障時にバックアップシステムを構築したりデータを再構築したりするのは困難かもしれない。モデルに問題が発見され、その問題が過去のモデルにも存在する場合 (例えば有害な入力に脆弱である場合)、新たに発見された問題にレジリエンスを</p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 悪意のある事象発生時にも防御運用を継続するため、モデル強化 (例: 敵対的訓練)、アンサンブル手法、信頼できるモデルバージョンへの自動フェイルオーバーなど、AI 固有のレジリエンスメカニズムを導入する。</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AI を活用したサイバー攻撃の速度と規模の拡大により、レジリエンス制御の実施が重要性を増している。</p> <p><b>参考情報例:</b> AI 100-2e2025</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	<p>各システムには固有の限界があり、それらは理解されている。これらの限界は適切な実装の指針となる。</p> <p><b>参考情報例：</b> NIST SP 800-53, Rev 5: CP; IR; SA08; SA-24; SC-06; SC-24; SC-36; SC39; SI-13;</p>	<p>持つ新モデルを作成・展開するのは容易ではないかもしれない。</p> <p><b>参考情報例：</b> DASF 3, 5, 19, 24, 34; OWASP 従来型ランタイム制御; OWASP AI Exchange: 一般的なガバナンス制御; OWASP モデル入力機密性; OWASP GenAI セキュリティプロジェクト: 監視; OWASP LLM トップ 10: LLM03 サプライチェーン; ENISA 脅威状況 2025; AI 1002e2025</p>	<p><b>参考情報例：</b> ENISA 脅威状況 2025 ; DASF 38,39 ; ATLAS AML.M0003 ; ATLAS AML.M0006 ; AI 100-2e2025</p>	
<p><b>PR.IR-04:</b> 可用性を維持するための十分なリソース容量を確保する</p>	<p><b>一般的な考察：</b> AI、特に深層ニューラルネットワークは、日常的に実行される最も計算負荷の高い作業の一つである。限られたリソースを最大限活用する戦略（負荷分散、キュー、並列処理など）は複数存在するが、重要なアプリケーションにおいては、これらの戦略には全て欠点がある。そのため、高可用性と低遅延応答を必要とするアプリケーションには、専用の計算インフラを用意することが適切である。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：CP-06 ; CP-07 ; CP-08 ; PM-03 ; PM-09</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 組織は AI リソースの必要性を考慮すべきである。AI ワークロードは非 AI 計算ワークロードよりも数桁以上リソース集約的である可能性があるためだ。</p> <p><b>参考情報例：</b> DASF 5、21、23-24、v30、34、45 ; OWASP AI Exchange : ガバナンス全般統制 ; OWASP LLM Top Ten : LLM03 サプライチェーン ENISA 脅威状況 2025 ; AI 100-2e2025</p>	<p><b>提案優先度：</b> 2</p> <p><b>機会例：</b> AI は防御態勢に影響する可能性のあるハードウェア障害やシステム劣化を予測する。</p> <p><b>重点領域の考慮事項例：</b> AI ワークロードはリソースを大量に消費するため、インシデント発生時には AI 防御行動用に計算リソースを確保しておく。</p> <p><b>参考情報例：</b> DASF 34,39,50 ; ENISA 脅威動向 2025 ; ATLAS AML.M0004 ; ATLAS AML.M0017 ; AI 100-2e2025</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> AI を活用した攻撃は、その攻撃が発生したか、あるいは発生しているかを適切に検知するために必要なリソースを増大させる可能性がある。これは特に、AI がサイバー防衛能力に実装される場合に重要である。その他の考慮事項については「防御」を参照のこと。</p> <p><b>参考情報例：</b> AI 100-2e2025</p>
<p><b>検知 (DE)</b></p>	<p>発生しうるサイバーセキュリティ攻撃や侵害を発見し分析する</p>			

CSF 2.0 コア	一般的な考慮事項		重点領域の優先事項と考慮事項	
			保護 (Secure)	防御 (Defend)
継続的監視 (DE.CM)	資産を監視し、異常、侵害の兆候、その他の潜在的な有害事象を発見する			
DE.CM-01: ネットワークとネットワークサービスは、潜在的に有害な事象を発見するために監視される	<p><b>一般的な考慮事項:</b> AIを導入する際、アプリケーションのセキュリティ確保や組織防衛にAIを活用する際に、新たな特有の考慮事項が生じる。</p> <p><b>参考情報例:</b> NIST SP 800-53、改訂5版: AC-02; AU-12; CA-07; CM-03; SC-05; SC-07; SI-04</p>	<p><b>提案優先度:</b> 2</p> <p><b>重点領域の考慮事項例:</b> AIシステムのトラフィックは、他のネットワークトラフィックとは別に追跡、記録、監視すべきだ。問題が発生した場合、その原因が人間によるものか AIによるものを容易に識別できる。</p> <p><b>参考情報例:</b> DASF 3-5、7、9-11、13、18-19、23-24、29-31、36、41、44-46、52、55-56、60、62; ATLAS AML.M0012; ATLAS AML.M0024; OWASP AI Exchange: 意図しない動作の影響を制限する制御; OWASP 従来型ランタイム制御; OWASP AI Exchange: 一般的なガバナンス制御; OWASP AI Exchange: モデルアクセス制御; OWASP GenAI Security Project: Monitor; OWASP AI Exchange: Rate Limit; OWASP LLM Top Ten: LLM03 サプライチェーン ENISA 脅威状況 2025; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度:</b> 1</p> <p>AIは監視を改善し、脅威検知を強化する。具体的には異常を検知し、不審な行動を関連付け、人間や他の自動化ツールよりも速く異常なパターンを発見する。</p> <p>AIエージェントは単独でもチームでも、ネットワークの監視、防御策の妥当性確認、検知精度の向上を行いながら、人間の作業負担を軽減できる。</p> <p>AIを活用してネットワークトラフィック（例: nmap スキャン実施）を自動追跡・監視し、潜在的な有害事象の検知を支援する。</p> <p>新たな監視・分析機能（例: ユーザーとマシンの行動分析、リアルタイム監視と対応）を活用し、組織が受動的な防御態勢から能動的な態勢（例: 予測分析）へ移行するのを支援できる AI 機能を識別する。</p> <p><b>重点領域の考慮事項例:</b> エージェントを監視・管理し、継続的な有効性を確保する。</p> <p><b>参考情報例:</b> DASF 25,32,39,61; ENISA 脅威状況 2025; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度:</b> 1</p> <p><b>重点領域の考慮事項例:</b> 標準のサイバーセキュリティ対策が適用される。追加のガイダンスについては「防御」を参照せよ。</p> <p><b>参考情報例:</b> <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<b>DE.CM-02:</b> 物理環境を監視し、潜在的に有害な事象を発見する	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53, Rev 5: CA-07; PE-03; PE-06; PE-20</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：OWASP AI Exchange：一般的なガバナンス管理策；ENISA 脅威状況 2025</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：AI システムはGPU クラスタや共有ラックに設置されることが多い。電力、発熱、物理的アクセスを監視せよ。これらの属性を改ざんされると防御機能が停止する恐れがある。</p> <p>参考情報例：DASF 32,39,41; ENISA 脅威状況 2025</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>
<b>DE.CM-03:</b> 人員の活動と技術の使用状況を監視し、潜在的に有害な事象を発見する	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂5版：AC-02；AU-12；AU-13；CA-07；CM-10；CM-11</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：内部および外部のAI ツールの人員による使用状況を監視し、有害事象や機密データの共有を発見すべきである。</p> <p>参考情報例：DASF 5, 7, 10-11, 13, 18-19, 23-24, 29, 33, 36, 41-42, 44-46, 52-53, 55, 64; ATLAS AML.M0024; OWASP AI Exchange: 不要な動作の影響を制限する制御; OWASP 従来型ランタイム制御; OWASP AI Exchange: 一般的なガバナンス制御; OWASP AI Exchange: モデルアクセス制御; OWASP GenAI セキュリティプロジェクト: 監視; OWASP LLM トップ 10: LLM03 サプライチェーン; ENISA 脅威状況 2025; AI 100-2e2025</p>	<p>提案優先度：3</p> <p>機会例：AI はアナリストが問題を解決するのを支援する。具体的には、一般的な問い合わせを処理し、アラートの要約を生成し、問題を適切なアナリストに振り分ける。</p> <p>AI エージェントは単独でもチームでも、ネットワークを監視し、防御措置の妥当性確認を行い、検知精度を向上させながら人的負担を軽減できる。</p> <p>AI は、異常な認証活動をフラグ付けすることで、ルールでは見逃される可能性のある認証情報の不正使用を検知する。</p> <p>重点領域の考慮事項例：標準のサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 25,37,39；ENISA 脅威状況 202；AI 100-2e2025</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：職員は AI を活用したフィッシング攻撃やディープフェイク攻撃の標的となり、システムにマルウェアが侵入する可能性がある。</p> <p>参考情報例： <a href="https://arxiv.org/pdf/2305.06972">https://arxiv.org/pdf/2305.06972</a>；AI 100-2e2025</p>
<b>DE.CM-06:</b> 外部サービスプロバイダの活	<p>一般的な考慮事項：一部の AI アプリケーションはサードパーテ</p>	<p>提案優先度：1</p>	<p>提案優先度：2</p>	<p>提案優先度：2</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<p>動とサービスは、潜在的に有害な事象を発見するために監視される</p>	<p>サービスに依存する場合があります。リクエスト、レスポンス、メタデータ、関連するメトリクスを表示するためにロギングを使用する。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：CA-07；PS07；SA-04；SA-09；SI-04</p>	<p><b>重点領域の考慮事項例：</b> 多くの組織は AI サービスについて外部プロバイダに依存している。このため、外部プロバイダ監視の重要性は依然として高い。これらのプロバイダを監視する方法は従来と変わらないため、AI 特有の考慮事項は存在しない。</p> <p><b>参考情報例：</b> DASF 7、10-11、13、18-19、29、36、41、44、52、60；ATLAS AML.M0024；OWASP 従来型ランタイム制御；OWASP AI Exchange: 一般的なガバナンス制御；OWASP GenAI セキュリティプロジェクト: 監視；OWASP LLM トップ 10: LLM03 サプライチェーン；ENISA 脅威状況 2025；AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>重点領域の考慮事項例：</b> 多くの防御ツールはサードパーティの AI API を呼び出す。これらの API は、潜在的に有害な事象を特定するために監視すべきである。</p> <p><b>参考情報例：</b> DASF 25,39,41；ENISA 脅威状況 2025；AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>重点領域の考慮事項例：</b> サードパーティのサービスやプロバイダは、ソフトウェアやシステムの更新やパッチによって新たな脆弱性を導入する可能性がある。AI を活用したサイバー攻撃は、こうした脆弱性を識別し悪用する恐れがある。さらに、サードパーティプロバイダの数が増えるほど、適切な管理や監視サービス・活動がなければ、AI を活用したサイバー攻撃が利用する脅威の規模も拡大する。</p> <p><b>参考情報例：</b> AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<p><b>DE.CM-09:</b> コンピューティングハードウェアとソフトウェア、実行環境、およびそれらのデータは、潜在的に有害な事象を発見するために監視される</p>	<p><b>一般的な考慮事項：</b> AI は自律的に動作するため、すべての内部 AI システムが異常な活動を適切に監視されていることを確認する。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AC-04；AC09；AU-12；CA-07；CM-03；CM-06；CM-10；CM-11；SC-34；SC-35；SI04；SI-07</p>	<p><b>提案優先度：</b> 1</p> <p><b>AI の重点領域の考慮事項例：</b> AI は自律的にデータを生成・拡張し、独自のコードを作成・実行できるため、AI の行動を追跡する新たな監視が必要となる AI システムへの入力と出力は、敵対的入力や異常な AI システム動作の監視など、有害事象を検知するために監視される可能性がある。人間が開始した AI 活動については、標準のサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 5、7-8、10-13、18-20、23-24、29-31、36、4-42、44-46、51-53、55-56、60；ATLAS</p>	<p><b>提案優先度：</b> 1</p> <p>AI は監視を改善し、脅威検知を強化する。具体的には異常をフラグ付けし、不審な行動を相関させ、人間や他の自動化ツールよりも速く異常なパターンを発見する。</p> <p>AI エージェントのチームがネットワークを監視し、防御措置の妥当性確認を行い、検知精度を向上させると同時に、人間の作業負担を軽減する。</p> <p><b>重点領域の考慮事項例：</b> AI システムとその実行環境を監視し、敵対的操作、データ漏洩、モデル悪用の兆候となる異常な動作（例：予期</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> AI を活用したサイバー攻撃は、目的達成のためにローカルコンピューティングリソースを利用する可能性がある。リソースおよび実行環境を監視し、異常な事象や有害な事象を検知する。</p> <p><b>参考情報例：</b> AI 100-2e2025； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		<p>AML.M0012; ATLAS AML.M0024; OWASP 制御：望ましくない動作の影響を制限する; OWASP 従来型ランタイム制御; OWASP AI Exchange：全般ガバナンス制御; OWASP AI Exchange：モデルアクセス管理; OWASP GenAI セキュリティプロジェクト：監視; OWASP LLM トップ 10：LLM03 サプライチェーン; ENISA 脅威状況 2025; AI 100-2e2025; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>せぬファイル書き込み、API 呼び出し、生成されたバイナリ) を検知する。</p> <p><b>参考情報例</b>：DASF 25,39,41 ; ENISA 脅威状況 2025 ; ATLAS AML.M0024 ; AI 100-2e2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	
<b>有害事象分析 (DE.AE)</b>	異常、侵害の兆候、その他の潜在的な有害事象を分析し、事象を特徴づけ、サイバーセキュリティインシデントを検知する			
<b>DE.AE-02</b> : 潜在的な有害事象を分析し、関連する活動をより深く理解する	<p><b>一般的な考慮事項</b>：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例</b>：NIST SP 800-53、改訂 5 版：AU-06 ; CA07 ; IR-04 ; SI-04</p>	<p><b>提案優先度</b>：2</p> <p><b>重点領域の考慮事項例</b>：敵対的入力事例など、AI システムに影響を及ぼす可能性のある有害事象を分析し、事象と関連活動の特徴付ける。</p> <p><b>参考情報例</b>：DASF 7, 12-14, 16, 19, 23, 29, 31, 35- 339, 42, 44, 46, 55-56, 59; OWASP 従来型ランタイム制御; OWASP AI エクスチェンジ：一般的なガバナンス制御; ENISA 脅威状況 2025</p>	<p><b>提案優先度</b>：2</p> <p>AI は監視を改善し、異常をフラグ付けし、不審な行動を関連付け、人間や他の自動化ツールよりも速く異常なパターンを発見することで脅威検知を強化する。</p> <p>AI は一般的な問い合わせの処理やアラート要約の生成、問題の適切なアナリストへの振り分けを行うことで、アナリストがより困難な問題解決に集中できるように支援する。</p> <p><b>重点領域の考慮事項例</b>：潜在的に有害な事象を分析する際には、AI 防御措置を補完し、ノイズ追跡を回避するために人間のレビューが必要だ。</p> <p><b>参考情報例</b>：ENISA 脅威状況 2025 ; DASF 25,32,39 ;</p>	<p><b>提案優先度</b>：2</p> <p><b>重点領域の考慮事項例</b>：AI 使用の指標となる潜在的な有害事象を分析することで、組織は AI を活用した脅威の可能性を理解できる。標準的なサイバーセキュリティ対策が適用される。追加ガイダンスについては「防御」を参照せよ。</p> <p><b>参考情報例</b>： <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
			<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	
<b>DE.AE-03:</b> 情報は複数の情報源から相関付けられる	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版：AU-06；CA07；PM-16；IR-04；IR-05；IR-08；SI04</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 7、12-14、16、19、23、29、31、35-37、39、42、44、46、55-56、59-60；ATLAS AML.M0024；OWASP Conventional Runtime Controls；OWASP AI Exchange: ガバナンス統制；ENISA 脅威状況 2025；<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>提案優先度：1</p> <p>AI は監視を改善し、脅威検知を強化する。具体的には異常を検知し、不審な行動を関連付け、人間や他の自動化ツールよりも速く異常なパターンを発見する。</p> <p>AI エージェントのチームがネットワークを監視し、防御措置の妥当性確認を行い、検知精度を向上させると同時に、人間の作業負担を軽減する。</p> <p>重点領域の考慮事項例：複数のログソースからのデータ集約は、異常かつ潜在的に有害な事象の検知において AI サイバー防御を強化する。</p> <p>参考情報例：ENISA 脅威状況 2025；DASF 32,39,41；<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティパッチが適用される。</p> <p>参考情報例：<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<b>DE.AE-04:</b> 不利な事象の推定影響と範囲は理解されている	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、Rev 5: PM-09；PM11；PM-18；PM-28；PM-30</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 13、16、19、23、31、39、56、59-60；OWASP AI Exchange：一般的なガバナンス管理策；OWASP LLM トップ 10：LLM03 サプライチェーン</p>	<p>提案優先度：1</p> <p>重点領域の考慮事項例：範囲の見積もりは、正確性を確認するため、人間のレビューによる生成的 AI データと照合すべきだ。</p> <p>参考情報例：DASF 32,39,41</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：AI を活用したサイバー攻撃の潜在的な範囲と規模を理解することで、組織は予防策とレジリエンス強化策の実施に有利な立場に立てる。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<b>DE.AE-06:</b> 障害発生に関する情報は、認可されたスタッフとツールにプロバイダされる	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版；IR-04；PM15；PM-16；RA-04；RA-10</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 7、12-14、16、19、23、29、35-39、42、44、46、55-56、59；ATLAS AML.M0024；ENISA 脅威状況 2025</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：有害事象に関連する AI の知見を、文脈と信頼度スコアを含めて説明し共有する。</p> <p>参考情報例：DASF 25,32,39；ENISA 脅威状況 2025</p>	<p>提案優先度：1</p> <p>重点領域の考慮事項例：AI を活用したサイバー攻撃は、サードパーティのプロバイダやツールに加え、複数のセキュリティチームやソフトウェアチームに影響を及ぼす可能性がある。優先順位付けと範囲を限定した対策を支援するため、全てのチームは有害事象を認識しておくべきだ。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>
<b>DE.AE-07:</b> サイバー脅威インテリジェンスやその他の文脈情報は、分析に統合されるべきである（ ）。	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版；PM-16；RA-03；RA-10</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 7、12-14、16、19、23、29、31、35-37、39、42、44、46、55-56、6061；OWASP AI Exchange: 一般的なガバナンス管理策；OWASP LLM Top Ten: LLM03 サプライチェーン； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>提案優先度：2</p> <p>AI は監視を改善し、脅威検知を強化する。<b>具体的には</b>、異常をフラグ付けし、不審な行動を関連付け、人間や自動化ツールよりも速く異常なパターンを発見する。</p> <p>AI は防御側に、膨大なデータセットをスキャンし、大量の脅威インテリジェンスを迅速に分析することで支援する。これにより防御側は脅威の状況を明確に把握できる。</p> <p>AI は標準プロトコル（STIX や OpenCTI など）を用いて脅威インテリジェンスを収集・フォーマット・共有し、チームやパートナー間の連携を確実にする。</p> <p>重点領域の考慮事項例：敵対的機械学習研究と AI レッドチーム報告書を検知パイプラインに組み込み、検知能力を強化し、対応と復旧活動を支援する。</p>	<p>提案優先度：1</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。追加ガイダンスについては「防御」を参照せよ。</p> <p>参考情報例： <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
			<b>参考情報例</b> : ENISA 脅威状況 2025、DASF 25、 <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	
<b>DE.AE-08</b> : インシデントは、有害事象が定義された  インシデント規準を満たす場合にインシデントとして宣言される	<b>一般的な考慮事項</b> : 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。  <b>参考情報例</b> : NIST SP 800-53, Rev 5: IR-04; IR-08	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : DASF 16、19、23、39、56、59 ; ENISA 脅威状況 2025	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : <b>DASF 25,32,39</b> ; ENISA 脅威状況 2025	<b>提案優先度</b> : 2  <b>重点領域の考慮事項例</b> : AI を活用したサイバー攻撃を宣言するための閾値を調整し、説明可能なエスカレーション規準を維持する。  <b>参考情報例</b> : AI 固有の参考情報例は追加情報待ち。
<b>対応 (RS)</b>	検知されたサイバーセキュリティインシデントに対する対応を実施する			
<b>インシデント管理 (RS.MA)</b>	検知されたサイバーセキュリティインシデントへの対応を管理する			
<b>RS.MA-01</b> : インシデント発生宣言後、関連するサードパーティと連携してインシデント対応計画を実行する	<b>一般的な考慮事項</b> : サードパーティのサービスおよびデータプロバイダと連絡を取る。  <b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : IR-06 ; IR-07 ; IR-08 ; SR-03 ; SR-08	<b>提案優先度</b> : 2  <b>重点領域の考慮事項例</b> : AI サービスにサードパーティが関与している場合、インシデント対応時には当該サードパーティと連携し、適切なインシデント対応活動が実施され、関係当事者間で適切に調整されるよう配慮することが適切である。データ漏洩に関連するインシデントについては、データの性質に応じて追加的な考慮事項が生じる場合がある（例 : 個人のプライバシーに影響を与える情報の漏洩は、各種プライバシー法規制に基づく漏洩通知義務を発生させる可能性がある）。  <b>参考情報例</b> : DASF 39 ; OWASP AI Exchange : ガバナンス統制 ; OWASP	<b>提案優先度</b> : 2  <b>機会例</b> : AI はトリアージや封じ込め手順の提案といったインシデント対応の自動化を支援し、チームがインシデント発生時により迅速かつ確信を持って行動できるようにする。  <b>重点領域の考慮事項例</b> : 防御的 AI の動作が外部 API やデータセットに依存する場合、インシデント発生時にはそれらのプロバイダと調整を行う必要がある。  <b>参考情報例</b> : DASF 25,39,41 ; ENISA 脅威状況 2025 ; AI 100-2e2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>	<b>提案優先度</b> : 2  <b>重点領域の考慮事項例</b> : AI を活用した攻撃が発生する速度と規模は、より迅速な対応と関連するサードパーティとの連携を必要とする。  <b>参考情報例</b> : AI 100-2e2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025 ; AI 100-2e2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a>		
<b>RS.MA-02:</b> インシデント報告はトリアージされ妥当性確認される	<p><b>一般的な考慮事項 :</b> AI 関連の報告および AI 関連の活動は、他の活動/報告とは別々に分類すべきである。</p> <p><b>参考情報例 :</b> NIST SP 800-53、改訂 5 版 : IR-04 ; IR-05 ; IR-06</p>	<p><b>提案優先度 :</b> 2</p> <p><b>重点領域の考慮事項例 :</b> AI は新たな脅威ベクトルと攻撃手法をもたらす。AI 関連インシデントのトリアージと妥当性確認規準を確立する。</p> <p><b>参考情報例 :</b> DASF 7、12-14、16、29、35-38、42、44、46、55-56、60 ; ENISA 脅威状況 2025</p>	<p><b>提案優先度 :</b> 1</p> <p><b>機会例 :</b> AI はトリアージなどのインシデント対応の自動化を支援し、封じ込め手順を推奨する。これによりチームはインシデント発生時により迅速かつ確信を持って行動できる。</p> <p><b>重点領域の考慮事項例 :</b> インシデントレポートは、対応時に AI を活用したサイバー防御措置が使用される可能性を反映するよう更新すべきだ。適切な措置が取られるよう、プロセスには人間のレビューと妥当性確認が含まれる。</p> <p><b>参考情報例 :</b> DASF 12,37,39; ENISA 脅威状況 2025</p>	<p><b>提案優先度 :</b> 2</p> <p><b>重点領域の考慮事項例 :</b> 標準的なサイバーセキュリティ対策が適用される。AI を活用した防御機能をインシデント対応パイプライン (インシデントデータの収集、報告書の作成・妥当性確認・プロバイダなど) に統合する際の追加ガイダンスについては、「防御」重点領域の考慮事項例を参照せよ。</p> <p><b>参考情報例 :</b> AI 固有の参考情報例は追加情報待ち。</p>
<b>RS.MA-03:</b> インシデントの分類と優先順位付け	<p><b>一般的な考慮事項 :</b> AI は、アプリケーションのセキュリティ確保時および組織防御に AI を活用する際に、新たな特有の考慮事項をもたらす。</p> <p><b>参考情報例 :</b> NIST SP 800-53、改訂 5 版 : IR-04 ; IR-05</p>	<p><b>提案優先度 :</b> 2</p> <p><b>重点領域の考慮事項例 :</b> AI は新たな脅威ベクトルと攻撃手法をもたらすため、この追加要素を捉える新たなインシデント分類を作成する必要がある。</p> <p><b>参考情報例 :</b> DASF 13、39 ; ENISA 脅威状況 2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度 :</b> 1</p> <p><b>重点領域の考慮事項例 :</b> AI 駆動型分析をインシデントの分類と優先順位付けに統合し、AI の影響を受けた事象 (例 : 敵対的攻撃、データ・ポイズニング) をリアルタイムで識別・フラグ付けする。</p> <p><b>参考情報例 :</b> DASF 25,39,41 ; ENISA 脅威状況 2025 ; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p><b>提案優先度 :</b> 1</p> <p><b>重点領域の考慮事項例 :</b> 標準的なサイバーセキュリティ対策が適用される。追加のガイダンスについては「防御」重点領域の考慮事項例を参照せよ。</p> <p><b>参考情報例 :</b> ATLAS AML.M0015; <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<b>RS.MA-04:</b> インシデントは必要に応じてエスカレーションまたはエスカレートされる	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版；IR-04；IR05；IR-06；IR-07</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 13、39；ENISA 脅威状況 2025</p>	<p>提案優先度：2</p> <p>機会例：AI は、インシデントをエスカレートまたはエベレーティングするタイミングに関する意思決定を支援できる。</p> <p>重点領域の考慮事項例：AI によるインシデント分類の結果を確認する。AI がインシデントを誤分類したり、その影響を過大評価したりした場合、早期にフラグを立て、人間のアナリストにエスカレーションする。</p> <p>参考情報例：DASF 25,32,39；ENISA 脅威状況 2025；ATLAS AML.M0017</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。（理由）AI を活用した防御に加え、システム遮断や隔離などの自動化措置を実施し、異常な行動や事象をフラグ付けして追加審査を行う。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>
<b>RS.MA-05:</b> インシデント復旧を開始する規準が適用される	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版；IR-04；IR-08</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 39；ENISA 脅威状況 2025</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：復旧には AI モジュールの再訓練または無効化が含まれる場合がある。AI コンポーネントをロールバックするトリガーを定義する。</p> <p>参考情報例：DASF 38,39；ENISA 脅威状況 2025；ATLAS AML.M0008；ATLAS AML.M0014； <a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。システム識別と復旧支援のための AI 導入など、追加ガイダンスについては「防御」を参照のこと。</p> <p>サイバーセキュリティ対策が適用される。システムの識別と復旧を支援する AI の実装など、追加ガイダンスについては「防御」を参照せよ。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>
<b>インシデント分析 (RS.AN)</b>	調査は、効果的な対応を確保し、フォレンジックおよび復旧活動を支援するために実施される			
<b>RS.AN-03:</b> 分析は、インシデント発生時の経緯と根本原因	<p>一般的な考慮事項：AI システムへの攻撃と防御の全体像を把</p>	<p>提案優先度：1</p>	<p>提案優先度：1</p>	<p>提案優先度：1</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
を特定するために行われる	<p>握するには、新たな分析ツールが必要となる可能性がある。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AU-07；IR04；SI-02(07)</p>	<p><b>重点領域の考慮事項例：</b> 敵対的入力など、AI に対するより複雑な攻撃を診断するには、新たな専門知識、ツール、手法が必要となる可能性がある。</p> <p><b>参考情報例：</b> DASF 39, 55；OWASP 標準ランタイム制御；ENISA 脅威状況 2025</p>	<p><b>重点領域の考慮事項例：</b> インシデント発生時に AI 固有のアーティファクト（例：モデルログ、推論テーブル、来歴証明データ）を分析し、根本原因を特定する。</p> <p><b>参考情報例：</b> DASF 21, 37；ATLAS AML.M0024</p>	<p><b>重点領域の考慮事項例：</b> インシデント分析では、インシデントにおける敵対者による AI 使用の指標を明示的に検索する。AI を活用した攻撃は、その速度と規模、動的かつ最適化された性質から、固有の指標や特徴を持つ可能性がある。敵対者による AI の使用は急速に進化しており、組織はインシデントで AI が使用されたか否か、またその使用方法を判断するために、サイバー脅威インテリジェンスを注意深く追跡する必要があるかもしれない。</p> <p><b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。</p>
<b>RS.AN-06:</b> 調査中に実施されたアクションは記録され、記録の完全性と来歴証明は保持される	<p><b>一般的な考慮事項：</b> 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版：AU-07；IR04；IR-06</p>	<p><b>提案優先度：</b> 3</p> <p><b>焦点領域の考慮事項の例：</b> 標準のサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 39, 55；OWASP 標準ランタイム制御；OWASP GenAI セキュリティプロジェクト；監視；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 25,39,41, ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> インシデント対応活動と知見は、将来のレジリエンス構築と全体的な改善努力を支援する（ID.IM-04 も参照）。</p> <p><b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。</p>
<b>RS.AN-07:</b> インシデントデータとメタデータは収集され、その完全性と来歴証明が保持される	<p><b>一般的な考慮事項：</b> AI は新たな種類のメタデータ（例：データバージョン、入力、ハイパーパラメータ）の取得をもたらす可能性がある。</p> <p><b>参考情報例：</b> NIST SP 800-53, Rev 5: AU-07; IR04; IR-06</p>	<p><b>提案優先度：</b> 1</p> <p><b>重点領域の考慮事項例：</b> AI の導入により、データセットの追跡とバージョン管理、およびモデルに関連するメタデータ（ハイパーパラメータなど）の文書化が必要となった。モデルのトレーニングに使用されたパラメータ、トレーニング時期、使用したデータセットのバージョンも関連する。</p>	<p><b>提案優先度：</b> 2</p> <p>AI システムのログ、入力、出力、意思決定の連鎖を保存し、の来歴証明を確保するとともに、将来の AI 駆動型対応行動を改善する。</p> <p><b>参考情報例：</b> DASF 25,39,41；ENISA 脅威状況 2025；ATLAS AML.M0024（AI テレメトリ記録）</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。詳細なガイドランスについては「防御に関する考慮事項」を参照のこと。</p> <p>サイバーセキュリティ対策が適用される。追加ガイドランスについては防御に関する考慮事項を参照のこと。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
		<p><b>参考情報例：</b>OWASP 標準ランタイム制御；OWASP GenAI セキュリティプロジェクト；監視；ENISA 脅威状況 2025</p>		<p><b>参考情報例：</b>AI 固有の参考情報例は追加情報待ち。</p>
<p><b>RS.AN-08:</b> インシデントの規模は推定され、妥当性確認される</p>	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b>NIST SP 800-53、改訂 5 版；IR-04；IR08；RA-03；RA-07</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 13、39；OWASP AI Exchange：一般ガバナンス管理；OWASP LLM トップ 10；LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> AI が影響したインシデントの規模を推定し、妥当性確認する。具体的には、モデルの完全性に対する敵対的影響の範囲、漏洩した機密データの量（例：トレーニングデータの漏洩）、およびモデル利用不能期間の長さを評価する。</p> <p><b>参考情報例：</b> DASF 25,32,41；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 2</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。実際のインシデントの規模を把握することで、将来のレジリエンス対策実施の優先順位が明確になる。追加のガイダンスについては防御の考慮事項を参照のこと。</p> <p><b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。</p>
<p><b>インシデント対応報告とコミュニケーション (RS.CO)</b></p>	<p>対応活動は、法令・規制・方針に基づき、内部および外部の関係者と調整される</p>			
<p><b>RS.CO-02:</b> 内部および外部の関係者にインシデントを通知する</p>	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p><b>参考情報例：</b> NIST SP 800-53、改訂 5 版；IR-04；IR-06；IR-07；SR-03；SR-08</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> DASF 7、12、14、29、35-37、39、42、46、55；OWASP AI Exchange：全般ガバナンス制御；OWASP LLM トップ 10；LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> AI 関連のインシデント（例：敵対的攻撃、予期せぬモデル障害）について通知プロセスを確立する。これにより、侵害されたモデルやデータなどのインシデントを内部チームや外部サプライヤーに迅速に伝達する。インシデント通知を自動的に配信できる場合と、事前に人間の確認が必要な場合の規準を設定する（例：法的またはコンプライアンス上の影響を及ぼす可能性のあるインシデントに関する通知は、送信前に人間の確認が必要となる場合がある）。</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b> 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例：</b> AI 固有の参考情報例は追加情報待ち。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
			<b>参考情報例</b> : ENISA 脅威状況 2025 ; DASF 25, 41 ; ENISA 脅威状況 2025 ATLAS AML.M0024 ;	
<b>RS.CO-03</b> : 情報は指定された内部および外部の関係者と共有される	<b>一般的な考慮事項</b> : 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。  <b>参考情報例</b> : NIST SP 800-53、改訂 5 版 ; IR-04 ; IR-06 ; IR-07 ; SR-03 ; SR-08	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : DASF 7、12、14、29、35-37、39、42、46、55 ; OWASP AI Exchange : 全般ガバナンス管理 ; OWASP LLM トップ 10 : LLM03 サプライチェーン ; ENISA 脅威状況 2025	<b>提案優先度</b> : 3  <b>機会例</b> : AI は明確なインシデント概要やコンプライアンス報告書のドラフト、証拠の整理、標準文書の生成を通じて報告を支援し、アナリストの作業負担を軽減する。  AI は脅威インテリジェンスを標準プロトコル (STIX や OpenCTI など) でフォーマットし共有する。これによりチームやパートナー間の連携を保つ。  AI は複雑な技術データを明確なビジネス言語に変換する。技術的リスクを簡潔な洞察に要約し、経営陣が情報に基づいたリスク判断を下せるよう支援する。  <b>重点領域の考慮事項例</b> : 協調的な防御強化のため、内部開発者や外部パートナーと AI 固有の脅威インテリジェンスやインシデント指標 (例 : 敵対的入力) を共有するプロトコルを確立する。  <b>参考情報例</b> : <b>DASF 25,32,41</b> ; ENISA 脅威状況 2025	<b>提案優先度</b> : 3  <b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。  <b>参考情報例</b> : AI 固有の参考情報例は追加情報待ち。
<b>インシデント緩和 (RS.MI)</b>	事象の拡大を防止し、その影響を緩和するための活動を実施する			

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<b>RS.MI-01:</b> インシデントは封じ込められる	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版；IR-04</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。(理由) AI が引き起こすインシデントは人間の対応速度を上回るため、その封じ込めの重要性が高まる。ただし、封じ込め手法自体は従来通りである。</p> <p>参考情報例：DASF 39；ENISA 脅威状況 2025； <a href="https://arxiv.org/pdf/2303.00654">https://arxiv.org/pdf/2303.00654</a></p>	<p>提案優先度：3</p> <p>機会例：AI はトリアージや封じ込め手順の提案といったインシデント対応の自動化を支援するため、チームはインシデント発生時により迅速に行動できる。</p> <p>重点領域の考慮事項例：封じ込め手順には、侵害された AI エージェントの自律性/特権を妥当性確認済みで信頼できる状態へ迅速に無効化するという、AI 固有のステップが含まれる。</p> <p>参考情報例：DASF 25,32,39,41；ENISA 脅威状況 2025</p>	<p>提案優先度：2</p> <p>重点領域の考慮事項例：AI を活用したサイバー攻撃は、検知を回避したり、検知を困難にする攻撃パターンを生成したりする可能性がある。システム内での AI 攻撃の拡散を防ぐため、システムを遮断または隔離する緩和を活用する。詳細は防御に関する考慮事項を参照のこと。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>
<b>RS.MI-02:</b> インシデントは根絶される	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53, Rev 5；IR-04</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 39；ENISA 脅威状況 2025</p>	<p>提案優先度：3</p> <p>機会例：AI は、トリアージや封じ込め手順の推奨など、インシデント対応の自動化を支援するため、チームはインシデント発生時により迅速に対応できる。</p> <p>重点領域の考慮事項例：根絶は、AI による侵害の根本原因に対処する。これには、汚染されたトレーニングデータの除去、脆弱な AI ライブラリのパッチ適用、敵対的ツールからのアクセス権限の完全な剥奪が含まれる。</p> <p>参考情報例：DASF 25,32,41；ENISA 脅威状況 2025</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>
<b>RECOVER (RC)</b>	サイバーセキュリティインシデントの影響を受けた資産と運用を復旧させる			

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<b>インシデント復旧計画の実行 (RC.RP)</b>	サイバーセキュリティインシデントの影響を受けたシステムとサービスの運用可用性を確保するため、復旧活動を実施する			
<b>RC.RP-01</b> : インシデント対応計画の復旧部分は、インシデント対応プロセスから開始されると同時に実行される	<p><b>一般的な考慮事項</b> : AI 関連のインシデントからの復旧は単純ではない場合がある AI には追加の考慮事項が必要となる場合がある復旧の複雑さは、攻撃の種類、モデルの種類、インシデントの深刻度によって異なる。最も単純なケースでは、バックアップからのデータ復元、ソフトウェアの更新、認証情報の更新で済む場合もある。より複雑なケースでは、組織はソフトウェアシステムの古いバージョンにロールバックする必要があるかもしれない。最も複雑なケースでは、モデルの再トレーニングが完全に必要となる可能性がある。</p> <p><b>参考情報例</b> : NIST SP 800-53、改訂 5 版 : CP-10 ; IR04 ; IR-08</p>	<p><b>提案優先度</b> : 2</p> <p><b>重点領域の考慮事項例</b> : AI システムの復旧作業には、他の種類のシステム (例 : モデルの再学習) の復旧作業では必要とされない複雑さが伴う可能性がある ( ) 。</p> <p><b>参考情報例</b> : DASF 39 ; ENISA 脅威状況 2025</p>	<p><b>提案優先度</b> : 2</p> <p><b>機会例</b> : AI は復旧を加速させる。復旧優先度の高いシステムを計算し、進捗を追跡し、関係者に状況を伝える明確な更新情報を にドラフトする。</p> <p>復旧活動の<b>重点領域の考慮事項例</b> : 復旧活動には、AI 関連のサイバー防御機能が信頼できる状態に戻ったかどうかの評価が含まれる。復旧にはモデルの再トレーニングや安全なチェックポイントへのロールバックが必要となる場合がある。</p> <p><b>参考情報例</b> : DASF 38,39,50; ENISA 脅威状況 2025; ATLAS AML.M0008; <a href="https://arxiv.org/pdf/2505.14835">https://arxiv.org/pdf/2505.14835</a></p>	<p><b>提案優先度</b> : 2</p> <p>復旧にはソフトウェアのパッチ適用や更新、パスワード変更、新規または更新されたアンチウイルスやファイアウォール保護のインストールが必要となる場合がある。</p> <p><b>参考情報例</b> : AI 固有の参考情報例は追加情報待ち。</p>
<b>RC.RP-02</b> : 復旧措置の選定、範囲設定、優先順位付け、および実施	<p><b>一般的な考慮事項</b> : 一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される。</p> <p><b>参考情報例</b> : DASF 39 ; ENISA 脅威状況 2025</p>	<p><b>提案優先度</b> : 1</p> <p><b>機会例</b> : AI は復旧すべきシステムを優先順位付けし、進捗を追跡し、関係者に状況を伝える明確な更新のドラフトを作成することで、復旧を加速させる。</p>	<p><b>提案優先度</b> : 3</p> <p><b>重点領域の考慮事項例</b> : 標準的なサイバーセキュリティ対策が適用される</p> <p><b>参考情報例</b> : AI 固有の参考情報例は追加情報待ち。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
	参考情報例：NIST SP 800-53、改訂 5 版：CP-10；IR04；IR-08		重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。 参考情報例：DASF 38,39,50；ENISA 脅威状況 2025	
<b>RC.RP-03:</b> 復元に使用する前に、バックアップやその他の復元資産の完全性を確認する	一般的な考慮事項：バックアップと過去のモデルに対して定期的なテストを実施し、概念のドリフトやその他のモデルの劣化を検知する。 参考情報例：NIST SP 800-53、改訂 5 版：CP-02；CP-04；CP-09	提案優先度：2 重点領域の考慮事項例：モデルデータがインシデントの原因となる場合がある。この場合、脆弱性を修正するためにデータの変更や追加が必要となる可能性がある。 参考情報例：DASF 8, 31, 41；ATLAS AML.M0012；AI 100-2e2025	提案優先度：2 重点領域の考慮事項例：モデルとデータセットのバックアップを汚染やドリフトに対してテストし、AI コンポーネントの完全性を保証する。 参考情報例：DASF 43,47；AI 100-2e2025	提案優先度：3 重点領域の考慮事項例：標準サイバーセキュリティ対策が適用される。追加のガイダンスについては防御上の考慮事項を参照のこと。 参考情報例：AI 特化参考情報例は追加情報待ち。
<b>RC.RP-04:</b> 重大なミッション機能とサイバーセキュリティリスクマネジメントは、インシデント発生後の運用基準を確立するために考慮される	一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。 参考情報例：NIST SP 800-53、改訂 5 版：PM-08；PM-09；PM11；IR-01；IR-08	提案優先度：3 重点領域の考慮事項例：標準的なサイバーセキュリティ慣行が適用される。 参考情報例：OWASP AI Exchange：全般ガバナンス管理策；OWASP LLM トップ 10；LLM03 サプライチェーン；ENISA 脅威状況 2025	提案優先度：2 機会例：AI は防御態勢に影響する可能性のあるハードウェア障害やシステム劣化を予測する。 重点領域の考慮事項例：インシデント発生後、AI 防衛システムの性能（例：検知精度、誤検知率）を評価し、AI が事後対応の運用規範を改善する方法を決定する。 参考情報例：DASF 39,50；ENISA 脅威動向 2025；OWASP AI Exchange：責任ある AI／信頼できる AI とは？；ATLAS AML.M0008；	提案優先度：2 重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。追加ガイダンスについては防御に関する考慮事項を参照のこと。 参考情報例：AI 固有の参考情報例は追加情報待ち。
<b>RC.RP-05:</b> 復旧した資産の完全性が検証され、システムとサー	一般的な考慮事項：一般的な考慮事項は識別されていない。	提案優先度：3	提案優先度：3	提案優先度：2 重点領域の考慮事項例：標準

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
<p>ビスが復旧し、正常な稼働状態が確認される</p>	<p>重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版；CP-10</p>	<p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 31</p>	<p><b>機会例：</b>AI は復旧対象システムの優先順位を計算し、進捗を追跡し、関係者に状況を伝える明確な更新情報のドラフトを作成することで、復旧を加速する。</p> <p><b>重点領域の考慮事項例：</b>復旧した AI コンポーネント（モデル、訓練データ）の完全性を検証し、侵害（例：残留ポイズニング）がないことを確認する。さらに、復旧した AI 防御システムが想定通りの性能（例：モデルの精度、誤検知率）で動作することを妥当性確認した上で、正常な運用状態を確認する。</p> <p>参考情報例：DASF 43,47; ATLAS AML.M0014; ATLAS AML.M0008; ENISA Theat Landscape 2025; <a href="https://arxiv.org/pdf/2505.14534v_1">https://arxiv.org/pdf/2505.14534v_1</a></p>	<p>サイバーセキュリティ対策が適用される。追加のガイダンスについては防御上の考慮事項を参照のこと。</p> <p>参考情報例：AI 特化参考情報例は追加情報待ち。</p>
<p><b>RC.RP-06:</b> インシデント復旧の終了は規準に基づいて宣言され、インシデント関連の文書化が完了する</p>	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版；IR-04; IR-08</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b>標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：ENISA 脅威状況 2025</p>	<p><b>提案優先度：</b> 3</p> <p><b>サンプル機会：</b>報告書の作成（例：事後報告書やクライアント監視出力の作成）。</p> <p><b>重点領域の考慮事項例：</b>文書化には AI 固有のアーティファクト（例：モデルログ、プロパティ記録）と、AI 防御システムの性能評価、および敵対的ベクトル（例：プロンプト・インジェクション）の緩和・撃退方法を詳細に記した最終事後検証報告書を含む。</p> <p>参考情報例：DASF 39,50; ATLAS AML.M0024; ATLAS AML.M0025; ENISA Theat Landscape 2025</p>	<p><b>提案優先度：</b> 3</p> <p><b>重点領域の考慮事項例：</b>標準</p> <p>サイバーセキュリティ対策が適用される。追加のガイダンスについては防御上の考慮事項を参照のこと。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>

CSF 2.0 コア	一般的な考慮事項	重点領域の優先事項と考慮事項		
		保護 (Secure)	防御 (Defend)	阻止 (Thwart)
インシデント復旧コミュニケーション (RC.CO)	復旧活動は内部および外部関係者と調整される			
<b>RC.CO-03:</b> 復旧活動および運用能力回復の進捗状況は、指定された内部および外部の関係者に伝達される	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版：IR-04；IR06；SR-08</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 31、39；OWASP AI Exchange：一般ガバナンス管理策；OWASP LLM トップ 10：LLM03 サプライチェーン；ENISA 脅威状況 2025</p>	<p>提案優先度：3</p> <p>機会例：AI は復旧すべきシステムを優先順位付けし、進捗を追跡し、関係者に状況を明確に伝える更新のドラフトを作成することで、復旧を加速させる。</p> <p>重点領域の考慮事項例：AI 関連の復旧時のコミュニケーションでは、関係者にモデルのステータス（例：復元されたモデルバージョン）と自動防御機能の再有効化までの予想遅延を伝える。</p> <p>参考情報例：ENISA 脅威動向 2025；DASF 39；<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：<a href="https://arxiv.org/html/2503.11917v3">https://arxiv.org/html/2503.11917v3</a></p>
<b>RC.CO-04:</b> インシデント復旧に関する公開情報は、承認された方法とメッセージングを用いて共有される	<p>一般的な考慮事項：一般的な考慮事項は識別されていない。重点領域の考慮事項例を参照のこと。</p> <p>参考情報例：NIST SP 800-53、改訂 5 版：CP-02；IR04；</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 31、39；ENISA 脅威状況 2025</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：DASF 25,32,39,41；ENISA 脅威状況 2025；ATLAS AML.M0002</p>	<p>提案優先度：3</p> <p>重点領域の考慮事項例：標準的なサイバーセキュリティ対策が適用される。</p> <p>参考情報例：AI 固有の参考情報例は追加情報待ち。</p>