共同サイバーセキュリティ情報





Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

AI システムを安全に導入する

セキュアでレジリエンスに優れた *AI* システムを導入するためのベストプラクティス

エグゼクティブサマリー

人工知能（AI）システムを安全に導入するには、AI システムの複雑さ、必要なリソース（資金、技術的専門知識など）、使用するインフラ（オンプレミス、クラウド、ハイブリッドなど）に応じて、慎重な設定と構成が必要である。本レポートは、安全な AI システム開発のためのガイドラインの「安全な導入」と「安全な運用と保守」のセクションを拡張し、「人工知能（AI）との関わり」における低減の考慮事項を組み込んだものである。これは、他の事業体が設計・開発した AI システムを導入・運用する組織向けのものである。ベストプラクティスはすべての環境に適用できるわけではないので、低減は特定のユースケースと脅威プロファイルに適合させる必要がある。[1], [2]

AI セキュリティは急速に発展している研究分野である。政府機関、産業界、学界が AI 技術の潜在的な弱点とそれを悪用するテクニックを発見するにつれて、組織は従来の IT のベストプラクティスを AI システムに適用するだけでなく、変化するリスクに対処するために AI システムを更新する必要がある。

本報告書は、米国国家安全保障局の人工知能セキュリティ・センター（AISC）、サイバーセキュリティ・インフラセキュリティ庁（CISA）、連邦捜査局（FBI）、オーストラリア信号長官のオーストラリア・サイバーセキュリティ・センター（ACSC）、カナダ・サイバーセキュリティ・センター（CCCS）、カナダ・サイバーセキュリティ・センター（CCCS）ニュージーランド国家サイバーセキュリティセンター（NCSC-NZ）、英国国家サイバーセキュリティセンター（NCSC-UK）によって認可された。

AISC と本報告書の目標は以下の通りである：

1. AI システムの機密性、完全性、可用性を改善する；
2. AI システムの既知のサイバーセキュリティ脆弱性が適切に低減されていることを保証する。

3. AI システムと関連するデータおよびサービスに対する悪意ある活動を保護、検知、対応するための方法論と管理者を提供する。

範囲と読者

本レポートにおける AI システムとは、機械学習（ML）ベースの人工知能（AI）システムを指す。

これらのベスト・プラクティスは、外部で開発された AI システムを構内やプライベート・クラウド環境で展開・運用する組織、特に脅威が高く、価値の高い環境にある組織に最も適用できる。これらのベストプラクティスは、自社で AI システムを導入せず、他者が導入した AI システムを活用している組織には適用できない。

ガイドラインのすべてが、すべての組織や環境にそのまま当てはまるわけではない。AI システムを標的にする敵対者によって、巧妙さのレベルや攻撃方法は異なるため、組織は自社のユースケースや脅威プロファイルと合わせてガイダンスを検討する必要がある。

AI システムの設計・開発面については、「安全な AI システム開発のためのガイドライン」を参照のこと。[1]

序文

AI 機能の急速な採用、導入、利用は、悪意のあるサイバー行為者にとって非常に貴重な標的となり得る。歴史的に機密情報や知的財産のデータ窃盗を利用して自分たちの利益を高めてきた行為者は、導入された AI システムを共用して悪意のある目的に適用しようとするかもしれない。

AI システムを標的とする悪意ある行為者は、従来の IT に対して使用される標準的な手法だけでなく、AI システム特有の攻撃ベクトルを使用する可能性がある。攻撃ベクトルは多種多様であるため、防御は多様かつ包括的である必要がある。高度な悪意ある行為者は、より複雑な操作を実行するために複数のベクターを組み合わせることが多い。このような組み合わせは、より効果的に多層防御を突破することができる。

組織は、導入環境の安全確保、AI システムの継続的な保護、AI システムの安全な運用と保守のために、以下のベストプラクティスを検討すべきである。

以下のベストプラクティスは、CISA と国立標準技術研究所（NIST）が策定した分野横断的なサイバーセキュリティ・パフォーマンス・ゴール（CPG）に沿ったものである。CPG は、CISA と NIST がすべての組織に導入を推奨する最低限のプラクティスと防御を提供するものである。CISA と NIST は、最も一般的で影響力のある脅威、戦術、技術、手順から保護するための既存のサイバーセキュリティのフレームワークとガイダンスに基づいて CPG を作成した。追加の推奨ベースライン防御を含む CPGs の詳細については、CISA の Cross-Sector Cybersecurity Performance Goals を参照されたい。

導入環境を保護する

組織は通常、既存の IT インフラ内に AI システムを導入する。導入に先立ち、強固なガバナンス、適切に設計されたアーキテクチャ、安全な構成など、IT 環境に健全なセキュリティ原則が適用されていることを確認する必要がある。例えば、AI システムのサイバーセキュリティの責任者及び説明責任者が、組織のサイバーセキュリティ全般の責任者及び説明責任者と同一であることを確認する[CPG 1.B]。

IT 環境におけるセキュリティのベストプラクティスと要件は、AI システムにも適用される。以下のベスト・プラクティスは、AI システムと、組織が AI システムを導入する IT 環境に適用することが特に重要である。

導入環境のガバナンスを管理する

- IT 部門以外の組織が AI システムを導入または運用している場合は、IT サービス部門と協力して導入環境を特定し、それが組織の IT 標準に適合していることを確認する。
    - 組織のリスクレベルを理解し、AI システムとその使用が、組織全体のリスク許容範囲内であり、AI システムをホストする特定の IT 環境のリスク許容範囲内であることを確認する。該当する脅威、潜在的な影響、リスクの受容をアセスメントし、文書化する。[3], [4]
    - 各ステークホルダーの役割と責任、およびそれを果たすための説明責任を特定する。これらのステークホルダーを特定することは、組織が IT 環境を識別システムとは別に管理している場合には特に重要である。
    - IT 環境のセキュリティ境界を特定し、その中で AI システムがどのように適合するかを特定する。
- AI システムの主要開発者に、そのシステムの脅威モデルの提供を求める。
    - AI システム導入チームは、セキュリティのベストプラクティスを実施し、潜在的な脅威を評価し、低減策を計画するための指針として、脅威モデルを活用すべきである。[5], [6]
- AI システム製品またはサービスの契約を策定する際には、導入環境のセキュリティ要件を考慮する。
- 特にデータサイエンス、インフラストラクチャー、サイバーセキュリティの各チームを含む関係者全員が協力的な文化を推進し、各チームがリスクや懸念を発言し、組織が適切に対処できるようにする。

堅牢な展開環境アーキテクチャを確保する

- IT 環境と AI システムの境界のセキュリティ防御を確立する [CPG 2.F]。
- 脅威モデルが識別した AI システムの境界防御及びその他のセキュリティ 関連領域における盲点を特定し、対処する。例えば，AI モデルが重み付けを行うアクセス制御システムを確実に使用し，二人制御（TPC） 及び二人完全性（TPI）[CPG 2.E]を有する特権ユーザのセットへのアクセスを制限する。

- AI モデルの学習や微調整に使用する、組織独自のデータソースをすべて特定し、防御する。他者がトレーニングしたモデルのデータソースのリストがある場合は、それを調べる。信頼できる有効なデータソースのカタログを維持することは、潜在的なデータ・ポイズニングやバックア・ポイズニング攻撃から保護するのに役立つ。サードパーティから取得したデータについては、CPG 1.G および CPG 1.H が推奨する契約またはサービスレベル合意（SLA）の規定を考慮する。
- セキュア・バイ・デザインの原則とゼロ・トラスト（ZT）フレームワークをアーキテクチャに適用し、AI システムとの間のリスクをマネジメントする。[7], [8], [9]

導入環境の設定を固める

- 導入環境に既存のセキュリティベストプラクティスを適用する。これには、ハード化されたコンテナまたは仮想マシン（VM）内で ML モデルを実行する環境のサンドボックス化 [CPG 2.E]、ネットワークの監視 [CPG 2.T]、許可リストによるファイアウォールの構成 [CPG 2.F]、および NSA のクラウド展開のためのクラウド低減戦略トップ 10 にあるようなその他のベストプラクティスが含まれる。
- ハードウェアベンダーのガイダンスや通知（GPU、CPU、メモリなど）を確認し、できれば共通セキュ リティアドバイザリフレームワーク（CSAF）を介して、脆弱性を悪用されるリスクを最小 化するためのソフトウェアパッチやアップデートを適用する。[10]
- 機密性の高い AI 情報（AI モデルの重み、出力、ログなど）は、静止時にデータを暗号化することで保護し、後でオンデマンドで復号化できるように暗号鍵をハードウェア・セキュリティ・モジュール（HSM）に保存する[CPG 2.L]。
- 強力な本人認証メカニズム、アクセス管理者、および安全な通信プロトコルを実装する。例えば、最新バージョンのトランスポート・レイヤー・セキュリティ（TLS）を使用して、転送中のデータを暗号化する [CPG 2.K]。
- 情報及びサービスへのアクセスに、フィッシングに耐性のある多要素認証（MFA）を確実に使用する。[2] 不正な本人認証の試みを監視し、対応する [CPG 2.H]。[11]
- 初期アクセスのために日常的に悪用される「脆弱なセキュ リティ対策」と「脆弱なセキュリティ対策」の低減策に従い、悪意ある行為者が脆弱なセキュ リティ対策を悪用する仕組みを理解し、それを低減する。

導入ネットワークを脅威から防御する

侵害は避けられない、またはすでに発生していると想定する ZT マインドセットを採用する。検知と対応の機能を導入し、侵害を迅速に特定して封じ込める。[8], [9]

- 十分にテストされた高性能のサイバーセキュリティソリューションを使用して、不正アクセスの試みを効率的に識別し、インシデント評価の速度と精度を高める [CPG 2.G]。

- インシデント検知システムを統合し、インシデントの優先順位付けを支援する [CPG 3.A]。また、迅速な対応が必要な重大インシデントが発生した場合、悪意があると疑われるユーザーのアクセスを即座にブロックしたり、AI モデルやシステムへのインバウンド接続をすべて切断したりする手段を統合する。

AI システムを継続的に保護する

モデルはソフトウェアであり、他のすべてのソフトウェアと同様に、脆弱性、その他の弱点、悪意のあるコードや特性を持つ可能性がある。

使用前と使用中に *AI* システムを検証する

- 暗号化手法、デジタル署名、チェックサムを使用して、各アーティファクトの出所と完全性を確認し（例えば、セーフセンサーを暗号化して完全性と機密性を保護する）、AI プロセス中の不正アクセスから機密情報を保護する。[14]
- AI モデルとシステムの各リリースのハッシュと暗号化されたコピーを作成し、改ざんできない場所に保管する。ハッシュ値および／または暗号化キーを安全な保管庫または HSM に保管し、暗号化キーと暗号化されたデータとモデルの両方に同じ場所でアクセスできないようにする。[1]
- すべての形式のコード（ソースコード、実行可能コード、コードとしてのインフラストラクチャなど）と成果物（モデル、パラメータ、コンフィギュレーション、データ、テストなど）を、適切なアクセス制御を備えたバージョン管理システムに格納し、検証済みのコードのみが使用され、あらゆる変更が追跡されるようにする。[1]
- AI モデルの堅牢性、正確性、修正後の潜在的脆弱性を徹底的にテストする。敵対的テストなどの技術を適用して、侵害の試みに対するモデルのレジリエンスを評価する。[4]
- AI システムの信頼性、効率性を高め、継続的デリバリーを可能にするために、自動ロールバックに備え、フェイルセーフとして人間がループに入る高度な導入メントを使用する。AI システムの文脈では、ロールバック機能は、新しいモデルやアップデートが問題を引き起こしたり、AI システムが危険にさらされたりした場合に、組織が迅速に最後の既知の良好な状態に戻し、ユーザーへの影響を最小限に抑えることを保証する。
- 外部の AI モデルやデータのサプライチェーンセキュリティを評価し、それらが組織の標準やリスクマネジメントポリシーに準拠していることを確認し、セキュアバイデザインの原則に従って開発されたものを優先する。組織の標準や方針を遵守できないサプライチェーンの部分については、リスクを理解し、受容できるようにする。[1], [7]

- エンタープライズ環境ですぐにモデルを実行しない。チューニング、学習、導入を検討する前に、安全な開発ゾーン内でモデル、特に輸入された事前学習済みモデルを注意深く検査する。導入前にモデルの妥当性を保証するために、潜在的な悪意のあるコードを検知するために、組織で承認された AI 専用スキャナが利用可能な場合は、そのスキャナを使用する。
- 検知、分析、対応の自動化を検討し、潜在的なサイバーインシデントへの迅速かつ的を絞った対応を可能にする洞察を与えることで、IT チームとセキュリティチームの効率化を図る。AI モデルとそのホスティング IT 環境を継続的にスキャンし、改ざんの可能性を特定する。
    - 自動化をより効率的にするために他の AI 機能を使うかどうかを検討する際には、リスクと利益を慎重に検討し、必要な場合には人間がループに入るようにする。

セキュアな *API* を公開する

- AI システムがアプリケーション・プログラミング・インターフェース（API）を公開する場合は、API アクセス用の認証および認可メカニズムを実装することによって、API を保護する。暗号化と本人認証を伴う HTTPS などの安全なプロトコルを使用する [CPG 2.C、2.D、2.G、2.H]。[1]
- 望ましくない、疑わしい、互換性のない、あるいは悪意のある入力が AI システムに渡されるリスク（プロンプト・インジェクション攻撃など）を低減するために、すべての入力データに対してバリデーションとサニタイズのプロトコルを実装する。[1]

モデルの行動を積極的に監視する

- 入力、出力、中間状態、エラーを網羅するログを収集し、アラートとトリガーを自動化する [CPG 2.T]。
- モデルのアーキテクチャとコンフィギュレーション設定を監視し、モデルのパフォーマンスやセキュリティーを損なうような不正な変更や予期せぬ変更がないか確認する。[1]
- AI モデルからデータにアクセスしたり、データを引き出したり、推論応答を集約しようとする試みを監視する。[1]

モデルの重みを防御する

- モデルの重みにアクセスするためのインターフェイスを強化し、敵対者が重みを流出させるのに要する労力を増加させる。例えば、API がタスクに必要な最小限のデータしか返さないようにして、モデルの反転を抑制する。
- 実現可能な限り、モデルウェイト保存のハードウェア防御を実装する。例えば、不要なハードウェアコミュニケーション機能を無効にし、発散やサイドチャンネル技術から防御する。

- 重量の保管を積極的に分離する。例えば、モデルウェイトを保護された保管庫、HRZ（Highly Restricted Zone：高度に制限されたゾー ン）（すなわち、別の専用エンクレーブ）、または HSM [CPG 2.L]に保管する。[12]

安全な AI の運用と保守

組織で承認された IT プロセスおよび手順に従って、承認された方法で AI システムを導入し、以下の管理が実施されていることを確認する。

厳格なアクセス制御を実施する

- AI モデルへの不正アクセスや改ざんを防止する。役割ベースのアクセス制御（RBAC）、可能であれば属性ベースのアクセス制御（ABAC）を適用し、認可された人員のみにアクセスを制限する。
    - ユーザと管理者を区別する。管理者アクセスには MFA と特権アクセスワークステーション（PAW）を要求する [CPG 2.H]。

ユーザーの意識向上およびトレーニングを確保する。

強固なパスワード管理、フィッシングの防止、安全なデータの取り扱いなど、セキュリティのベストプラクティスについて、ユーザー、管理者、開発者を教育する。人為的ミスのリスクを最小化するために、セキュリティを意識する文化を促進する。可能であれば、クレデンシャル・マネジメント・システムを使用してクレデンシャルの使用 を制限、管理、監視し、リスクをさらに最小化する［CPG 2.I］。

監査と侵入テストの実施

- 外部のセキュリティ専門家を活用し、すぐに導入可能な AI システムの監査と侵入テストを実施する。これにより、社内で見落とされている脆弱性や弱点を特定することができる。[13], [15]

堅牢なロギングとモニタリングを導入する

- 異常な動作や潜在的なセキュリティインシデントを検知するために、堅牢な監視及びログの仕組みにより、システムの動作、入力及び出力を監視する [CPG 3.A]。[16] データのドリフト、高頻度又は反復的な入力を監視する（これらは、モデルの危殆化又は自動的な危殆化の試みの兆候である可能性があるため）。[17]
- オラクル式の潜在的な敵対的侵害の試み、セキュリティ侵害、または異常を管理者に通知する警告システムを確立する。AI システムを保護するためには、サイバーインシデントをタイムリーに検知し対応することが重要である。[18]

定期的にアップデートし、パッチを当てる

- モデルを新しい／異なるバージョンに更新するときは、再展開する前に、完全な評価を実行し、精度、性能、セキュリティテストが許容範囲内にあることを確認する。

高可用性（*HA*）と災害復旧（*DR*）の準備

- システムの要件に応じて、不変バックアップストレージシステムを使用し、すべてのオブジェクト、特にログデータが不変であり、変更できないようにする[CPG 2.R]。[2]

安全な削除機能を計画する

- データやモデルが公開またはアクセス可能なあらゆるプロセスの完了時に、トレーニングモデルや検証モデル、暗号鍵などのコンポーネントを、いかなる残存物も保持することなく、自律的かつ復元不可能に削除する。[19]

結論

認可機関は、AI システムを導入する組織に対し、機密データの盗難を防止し、AI システムの悪用を低減することができる強固なセキュリティ対策を導入するよう助言している。例えば、ディープニューラルネットワークの学習可能なパラメータであるモデルの重みは、特に保護すべき重要な要素である。これは、高度な AI モデルを学習させるための、膨大な計算リソース、収集・処理された、潜在的に機密性の高い学習データ、アルゴリズムの最適化など、多くのコストと困難な前提条件の結果である。

AI システムはソフトウェア・システムである。そのため、導入する組織は、AI システムの設計者や開発者が、運用開始後のシステムのセキュリティ上の成果に積極的な関心を持つような、設計上安全なシステムを好むべきである。[7]

重大なセキュリティ・ギャップを避けるためには、関連するすべての攻撃ベクトルに対するセキュリティ対策を包括的に実施することが必要であり、ベスト・プラクティスは AI の分野や技術の進化とともに変化していくだろうが、以下に特に重要な対策をまとめる：

- 特権アクセスが使用される、または重要なサービスが実行されるすべてのデバイスについて、継続的な危殆化評価を実施する。
- IT 導入環境を強化し、更新する。
- AI モデルとサプライチェーン・セキュリティの源を見直す。
- 導入前に AI システムを検証する。
- 最小特権と深層防御の概念を採用し、AI システムの厳格なアクセス制御と API セキュリティを実施する。

- 堅牢なロギング、モニタリング、ユーザーおよび事業体行動分析（UEBA）を使用して、内部脅威やその他の悪意のある活動を特定する。
- モデルの重みは AI システムの本質であるため、モデルへのアクセスを制限し保護する。
- 特に急速に進化している AI 分野において、現在および新たな脅威に対する認識を維持し、組織の AI システムがセキュリティギャップや脆弱性を回避するために強化されていることを確認する。

結局のところ、AI システムの安全確保には、リスクを特定し、適切な低減策を実施し、問題がないか監視する継続的なプロセスが必要である。AI システムの導入と運用を安全にするために、本レポートで説明したステップを踏むことで、組織はリスクを大幅に軽減することができる。これらの手順は、組織の知的財産、モデル、データを盗難や悪用から守るのに役立つ。

最初から優れたセキュリティ対策を実施することで、AI システムの導入を成功させるための正しい道を歩むことができる。

引用文献

[1] National Cyber Security Centre et al. 安全な AI システム開発のためのガイドライン.2023. https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf

[2] Australian Signals Directorate et al. Engaging with Artificial Intelligence (AI).2024. https://www.cyber.gov.au/sites/default/files/2024-01/Engaging%20with%20Artificial%20Intelligence%20%28AI%29.pdf

[3] MITRE.ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) Matrix version 4.0.0. 2024. https://atlas.mitre.org/matrices/ATLAS

[4] 国立標準技術研究所.AI リスクマネジメントフレームワーク 1.0.2023. https://www.nist.gov/itl/ai-risk-management-framework.

[5] オープン・ワールドワイド・アプリケーション・セキュリティ・プロジェクト（OWASP® ）。LLM AI サイバーセキュリティとガバナンスチェックリスト。https://owasp.org/www-project-top-10-for-large-language-model applications/llm-top-10-governance-doc/LLM_AI_Security_and_Governance_Checklist-v1.pdf.

[6] オープン・ワールドワイド・アプリケーション・セキュリティ・プロジェクト（OWASP® ）。OWASP Machine Learning Security Top Ten Security Risks.2023. https://owasp.org/www-project-machine-learning-security top-10/

[7] サイバーセキュリティ・インフラセキュリティ庁.セキュア・バイ・デザイン.2023. https://www.cisa.gov/securebydesign

[8] 国家安全保障局。ゼロ・トラスト・セキュリティ・モデルの導入。2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

[9] サイバーセキュリティ・インフラセキュリティ庁.ゼロトラスト成熟度モデル。2022. https://www.cisa.gov/zero-trust-maturity-model

[10] サイバーセキュリティ・インフラセキュリティ庁.脆弱性管理の状況を変革する。2022. https://www.cisa.gov/news-events/news/transforming-vulnerability management-landscape

[11] サイバーセキュリティ・インフラセキュリティ庁.フィッシングに強い MFA の実装.2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant mfa-508c.pdf

[12] カナダ・サイバーセキュリティセンター。ネットワークセキュリティゾーンのベースラインセキュリティ要件 Ver.2.0 (ITSP.80.022)。2021. https://www.cyber.gc.ca/en/guidance/baseline-security requirements-network-security-zones-version-20-itsp80022

[13] ジ ジェシカ AI レッドチームとは何を意味するのか？https://cset.georgetown.edu/article/what-does-ai-red-teaming-actually-mean/。

[14] ハグする顔 GitHub.セーフセンサー。2024. https://github.com/huggingface/safetensors.

[15] マイケル・フェファー、アヌーシャ・シンハ、ザッカリー・C・リプトン、ホーダ・ハイダリ。生成的 AI のためのレッドチーム：銀の弾丸かセキュリティ劇場か？2024. https://arxiv.org/abs/2401.15897

[16] グーグルグーグルのセキュア AI フレームワーク（SAIF）。2023. https://safety.google/cybersecurity advments/saif/

[17] 政府アカウンタビリティ室（GAO）。人工知能：連邦政府機関およびその他の事業体のための説明責任の枠組み。2021. https://www.gao.gov/assets/gao-21-519sp.pdf

[18] リスクインサイト AI を攻撃する？実例だ！.2023. https://riskinsight wavestone.com/ja/2023/06/attacking-ai-a-re-life-example

[19] 国立サイバーセキュリティセンター機械学習のセキュリティのための原則.2022. https://www.ncsc.gov.uk/files/Principles-for-the-security-of-machine-learning.pdf

推薦の免責事項

本文書に含まれる情報および意見は、「現状のまま」提供されるものであり、いかなる保証も行わない。本書に記載されている、商号、商標、製造事業者、その他による特定の商用製品、プロセス、またはサービスへの言及は、米国政府による推奨、推薦、または支持を意味するものではなく、本ガイダンスを広告または製品推奨の目的で使用してはならない。

目的

本文書は、脅威の識別と普及、サイバーセキュリティ仕様と緩和策の策定と発行といった認可機関の責務を含む、サイバーセキュリティの使命を推進するために作成された。この情報は、すべての適切な利害関係者に届くよう、広く共有される可能性がある。

連絡先

米国の組織である：

NSA サイバーセキュリティレポート フィードバック：CybersecurityReports@nsa.gov

NSA サイバーセキュリティに関する一般的な問い合わせまたは顧客からのリクエスト：Cybersecurity_Requests@nsa.gov

防衛産業基盤に関するお問い合わせとサイバーセキュリティサービス：DIB_Defense@cyber.nsa.gov

NSA メディアお問い合わせ／プレスデスク 443-634-0721, MediaRelations@nsa.gov

インシデントや異常な活動を CISA 24/7 オペレーションセンター（report@cisa.gov または (888) 2820870）、および/または最寄りの FBI 支局を通じて FBI に報告する。

オーストラリアの組織詳細情報またはサイバーセキュリティインシデントの報告については、cyber.gov.au をご覧になるか、1300 292 371（1300 CYBER1）までお電話を。

カナダの組織詳細については、サイバーセンター（contact@cyber.gc.ca）に連絡するか、サイバーセキュリティインシデントをポータルサイト（https://www.cyber.gc.ca/en/incident-management）に報告する。

ニュージーランドの組織サイバーセキュリティインシデントを incidents@ncsc.govt.nz に報告するか、04 498 7654 に電話する。**英国の組織**重要なサイバーセキュリティインシデントを ncsc.gov.uk/report-an-incident（24 時間監視）で報告するか、緊急の場合は 03000 200 973 に電話する。