スーパーコンピュータ「富岳」

セキュリティホワイトペーパー

理化学研究所 計算科学研究センター

2021 年 7 月

1　はじめに

理化学研究所計算科学研究センター（以下「センター」）はスーパーコンピュータ「富岳」（以下「富岳」）を可用性と信頼性の高いサービスとして提供することを目標としています。セキュリティに関しては、物理的な施設の保護、ネットワークの保護、データ保護、インシデント対応など情報セキュリティマネジメントシステム(ISMS)を参考に、包括的なセキュリティ管理プロセスを形成しています。本書では富岳のセキュリティに関する取り組みと、利用者がセキュリティについて考慮すべき点について説明します。

2　共有セキュリティ責任

「富岳」では、センターと利用者の間で役割を明確化したセキュリティの責任共有モデルを採用しています。センターは、「富岳」の計算機本体、ストレージ、ソフトウェア、ネットワーク、および「富岳」の設置されている施設のセキュリティ保護を管理し、責任を負います。 利用者は、自身の情報、データ、ユーザーアカウント、資格情報を管理する責任があります。

2.1　センターの責任範囲

センターは、「富岳」の計算機本体やストレージシステムなどのハードウェア、および「富岳」を構成するシステムソフトウェアやセンターが導入したアプリケーションなどを管理する責任を負います。また、外部とのネットワークや、施設設備の運用管理もセンターの責任です。

センターは、次の項目に重点を置いて管理しています。

物理的施設へのアクセス
ネットワークの管理
インフラストラクチャーの保護
システムソフトウェアの管理
データの保護

2.2　利用者の責任範囲

「富岳」の利用者は、以下の管理が求められます。

アカウントの適切な管理（登録・削除依頼、管理権限設定の付与など）
資格情報の管理
データの管理

3　プラットフォームのセキュリティ

センターの施設設備は、「富岳」を運用するために物理的および環境的なセキュリティを

確保するように設計されています。センターの施設には警備員が常駐しており、入館者はアクセスカード（ID カード）の着用が求められます。また、ビデオ監視システムでセンター内外が監視されています。「富岳」の設置されている計算機室と職員の執務エリアは明確に分離されており、入室権限をもつ一部の職員のみが計算機室に入室できます。建物自体には各種災害対策が施されており、「富岳」の運用を継続できる仕組みを備えています。

3.1 防犯監視体制

入退室管理

センター内は、ID カードと電気錠を使った入退出管理システムで制御しています。建物への入退出をはじめ、特定のエリアには許可された者のみが入室でき、その他の人の入室を制限・禁止します。また、いつ誰が、どのエリアに入室をしたかの履歴を記録し、管理しています。

防犯設備とビデオ監視システム

センター全体の防犯設備、監視体制および監視室を有しています。ビデオ監視システムはセンターの建物内はもちろん、敷地内も監視対象とし、各室出入口および計算機室までの入館者の動線に添って設置しています。24 時間 365 日記録し、録画データは長期間保存しています。

警備員の配置

建物の入り口には警備員が常駐しており、来訪者の確認（身元確認、事前登録、担当者への連絡など）を行います。すべての来訪者は、専用ストラップのついた ID カードの着用が求められます。

3.2 災害対策

地震対策

センターは免震構造または耐震構造の建物であり、大規模地震に対してもセンターの機能を維持する構造となっています。

水害・塩害対策

センターは想定最高津波水位より高い地盤高で造成された立地（海抜 6m）に設けられているため、水害や津波の恐れが低い地域となります。また、海岸線近くの立地による塩害への対策として、壁や窓の二重化や、外気取込口への塩害除去フィルターを設置しています。

火災対策

センター内は自動火災報知設備を備えています。特に、「富岳」が設置されている計算機室および電気室には超高感度煙感知器および初期消火用として粉消火器や炭酸ガス消火器を設置しています。

落雷対策

センターは直撃雷および側雷の対策をしています。

電源設備

センターは変電所から二本の高圧送電線による給電ルートを確保しています。また、ガスタービンによる自家発電設備を常時稼働しているほか、UPS および非常用発電機も設置しており、瞬低時や停電時においても重要設備への継続的な電力供給を安定的に行うことを可能としています。

4 運用のセキュリティ

利用者が「富岳」の計算資源を安心して使用するために、センターではセキュリティプロセスに関する業界のベストプラクティスに従って、次のような運用を行っています。

最小限の特権管理
安全なネットワークおよびシステム環境
利用者データの管理
定期的な脆弱性スキャン
運用監視のログ記録とアラート
システム変更管理
セキュリティインシデントへの対応と復旧手順の確立

4.1 アクセス管理

利用者アカウントのアクセス管理

利用者アカウントの作成やアクセス権限に関する操作は、権限を適切かつ厳密に管理するために手順が確立されています。利用者アカウントには有効期限が設定されており、期限の切れたアカウントは随時停止処置を行います。利用者アカウントの権限はシステムを利用可能な最小限の権限に設定されています。

技術的なアクセス管理

利用者は PKI（公開鍵基盤）を使い、ウェブ(HTTPS)またはシェル(SSH)を用いて「富岳」に接続できます。また、利用者と「富岳」の間を仮想プライベートネットワーク(VPN)で接

続し、暗号化されたトンネル経由で「富岳」に接続できます。

「富岳」の認証局やホストの秘密鍵は、キーを保護するためのセキュリティポリシーと手順により安全に管理されています。

4.2 ネットワークセキュリティ

ネットワークセキュリティは、物理的制御と論理的制御の組み合わせを使用して実施しています。ファイアウォール、ネットワーク脆弱性スキャン、ネットワークセキュリティ監視などのネットワークセキュリティと監視技術により、悪意のある通信に対する保護と防御を実施しています。

センターのネットワークは、用途に基づきセグメント化されています。主要なネットワークは次のとおりです。

インターネット接続 DMZ
「富岳」のネットワーク
センターの一般業務イントラネットワーク

ネットワークの分離

センターの一般業務で使用するイントラネットと「富岳」のネットワークは完全に分離されており、相互に通信することはできません。また、無許可の機器や人員によるネットワーク接続を防止するために必要な制御を行っています。

ファイアウォール

富岳では、インターネットとのインバウンド・アウトバウンド通信の監視と制御を実施するためにファイアウォールを導入しています。外部ネットワークからの通信は基本的にすべて拒否され、「富岳」でサービスとして提供する通信のみが変更管理手順とセキュリティ監査を実施した上で許可されます。「富岳」から外部への通信は基本的にすべて許可されます。

通信セキュリティ

「富岳」へのアクセスには SSH または HTTPS プロトコルが利用できます。また「富岳」のネットワークへの VPN サービスも提供しています。強力な暗号化プロトコルの下で安全な通信を確保し、機密データの暗号化に対応しています。

4.3 データ管理

「富岳」の利用契約の終了に伴う利用者のデータ消去プロセス、および機器の故障等により IT 資産を確実かつ安全に処分する際の機密保護対策を含めた廃棄プロセスが定義されています。

データの保存

利用者のデータは冗長性(RAID6)を持つストレージに格納しています。

データの消去

課題実施期間終了日から一ヶ月後に課題に割り当てたデータ領域を消去します。消去後にデータは一切復元できません。

データのバックアップ

利用者のデータのバックアップは一切行いません。必要に応じて利用者自身でデータのバックアップを採取してください。

データの暗号化

ストレージ上の利用者のデータは暗号化されません。

4.4 脅威・脆弱性管理

脅威を効果的かつ正確に検出するためのシステム管理手順が設けられています。また脆弱性の情報は随時入手し、「富岳」へのリスクを分析し対処しています。

脆弱性スキャン

センターは、「富岳」のネットワークに対して定期的なスキャンを実施し、未許可なサービスの検出およびリスクの高いセキュリティの脅威と脆弱性の有無を確認しています。リスクの高いサービスを発見した場合にはセキュリティパッチを適用します。

セキュリティパッチ管理

「富岳」では、セキュリティパッチを安全および迅速に適用するためにパッチ管理手順を設けています。すべてのサーバおよびネットワーク機器へのパッチは、システムの安定性に対するパッチの影響を分析した上で適用します。緊急性の高い脆弱性に対しての重要なパッチは迅速に適用し、その他のパッチは適用可否を判断した上で計画保守に合わせて適用します。

4.5 運用監視

ログ監視

「富岳」では、サービスを維持するための各機器(物理ホスト、ネットワーク、ストレージ等)に対して、さまざまな自動監視システムを活用することで、高い可用性を提供しています。重要なログは日々確認しており、問題があればエスカレーションし解決を図ります。

死活監視

各機器およびサービスに対して一定間隔のチェックを自動的に行い、障害時に運用担当者にアラート通知をします。「富岳」を構成する重要なシステムの多くは二重化されており、全体としての可用性を確保しています。

パフォーマンス監視

各機器およびサービスの性能情報を計測し、一定時間しきい値を超過した場合に運用担当者にアラート通知をします。また、原因を調査し、要因の除去あるいはシステムの拡張を含む対策を行います。また、運用監視システムによって、物理的な環境変化やパーツの故障・劣化等に関する情報を運用担当者に通知することで、性能の低下を防止しています。

リソース監視

各機器およびサービスのリソース使用率を計測し、しきい値を超過した場合に、運用担当者にアラート通知をします。また、超過の原因を調査し、要因の除去あるいはリソースの拡張を検討します。

4.6 システム変更管理

すべてのシステム変更はセキュリティ要件を満たすことを確認して実施しています。

システムへの変更手順

システムの変更手順は定義されており変更管理プロセスに則り許可された運用担当者のみが実施できます。すべての変更は承認プロセスを経て実施および記録しています。変更による問題が発生した場合に備え、復旧手順をあらかじめ作成しています。パッチを含むシステムへの変更は、テスト環境で動作確認後に本番環境へ適用します。

利用者への通知

センターは、利用者に影響を与える可能性のあるシステム変更について富岳ウェブサイトにて情報を提供します。提供する情報は以下となります。

システムの変更についての説明
変更予定日時および変更実施日時

4.7 インシデント管理

インシデント対応

インシデント発生時には、理化学研究所の定める情報セキュリティ実施手順に従い所内の CSIRT あるいは関連部署と連携し対応します。また、「富岳」は High-Performance

Computing Infrastructure(HPCI)にも計算資源を提供しており、HPCI のインシデント対応部署とも連携し対応します。

なお、センターが情報セキュリティインシデントの状況を追跡するため、利用者に協力を求める場合があります。その場合は別途方法・手段等をお知らせいたします。また、サービスに影響しない軽微なインシデントを含め、インシデント発生の情報を記録し再発防止に努めています。

インシデント通知

インシデント発生時には、事前に定められた対応手順に基づき関係者への情報伝達を行い、調査・対応します。また、利用者には基準に基づきインシデント情報をウェブサイトやメールにて開示します。

インシデント検知時の報告先

利用者が「富岳」の利用においてインシデントを検知した際には、富岳ウェブサイトの「お問い合わせ先」までご連絡下さい。

5 プライバシーと順守

「富岳」の利用者のプライバシーおよびデータについて、各種文章を定めこれら基準に従ってデータを取扱っています。

5.1 データプライバシー

「富岳」におけるデータの取扱について、以下の 2 つの文章で公開しています。

「スーパーコンピュータ「富岳」でのデータ等の取扱について」

https://www.hpci-office.jp/materials/f_guidelines_for_users_data_a_jp.pdf

「富岳」の利用者のファイルおよびセンターが収集するデータの取扱について定めています。

「スーパーコンピュータ「富岳」での個人に関するデータの取扱について」

https://www.hpci-office.jp/materials/f_guidelines_for_users_data_b_jp.pdf

「富岳」の利用者の個人情報およびアクセスログの取扱について定めています。

5.2 セキュリティ監査

内部監査体制

理化学研究所のセキュリティ担当部署により「富岳」のネットワークサービスについて定

期的に脆弱性の監査を行っています。

第三者による監査

外部機関による運用およびセキュリティに関する監査を定期的に実施しています。監査結果によってリスクが発見された際は、優先度に基づいて改善に向けた対策を実施します。

6　まとめ

本書では、理化学研究所計算科学研究センターが提供するスーパーコンピュータ「富岳」を信頼性と可用性の高い計算サービスとして利用者に安心してお使い頂くために、センターのセキュリティに関する取り組みについて説明しました。物理的な施設の保護、ネットワークの保護、データ保護、インシデント対応など情報セキュリティマネジメントシステム(ISMS)を参考に、センターでは包括的なセキュリティ管理プロセスを形成しています。また、物理的・技術的・管理面において徹底したセキュリティの確保に努めることで、安全に計算資源を提供するとともに、利用者が必要とするセキュリティ対策を実現しています。