第2回全ゲノム解析等の推進に関する専門委員会	資料
令和3年5月31日	3

解析・データセンター構築の詳細要件（案）

１．情報管理

（１）ガイドライン等の適応に関する留意事項

・統一基準群においては、「政府機関等の情報セキュリティ対策のための統一基準」だけではなく、「政府機関等の対策基準策定のためのガイドライン」に記載されている管理事項や対策手段についても導入すること。
・「医療情報システムの安全管理に関するガイドライン」の遵守にあたっては、A.制度上の要求事項、B.考え方、C.最低限のガイドライン、D.推奨されるガイドライン、いずれの対策内容も把握し遵守すること。
・システム構築の責任者や情報セキュリティ管理者は、上述のガイドライン等の遵守にあたり、情報管理者やシステム開発者の恣意的な解釈によって形骸化することのないように、常に確認すること。
・本事業において解析やデータセンターの維持に関わる職員は、定期的にデータ管理に関する自己点検を行うとともに、セキュリティ対策の専門家によるシナリオによりセキュリティ対策訓練を行うこと。

（２）情報へのアクセス監視に関する遵守事項

・データへのアクセス状況の証跡管理は、システムやアプリケーション、データベース等の構成技術に関するログだけでなく、ラボラトリー情報管理システム（LIMS）を活用し、誰が、どのデータを用いて解析等を行ったかも管理すること。
・不正アクセスの挙動監視は、ネットワークだけでなく、標的型攻撃の恐れがあるシステム全体の挙動や不審なデータアクセスに関する挙動まで自動的に検知し、監視すること。
・データ侵害等のリアルタイムな監視は、監視対象とのログ取得のインターフェースを多く保有し、相関分析等によりリスクを把握する SIEM（Security Information and Event Management）による人的な監視と、セキュリティ攻撃や不正アクセスの疑いに関して自動的にリスク判定ができる機械による監視を併用すること。
・ゼロトラストセキュリティの概念に基づき、情報へのアクセスは、電子証明書を活用して管理すること。

２．システム構築

（１）クラウド基盤利用に関する遵守事項

・クラウドの構成は、特定のクラウドサービスに依存せず、複数のクラウドサービスの特性を比較検討し、適材適所にクラウドサービスを配置すること。特定のクラウドサービスのみの採択は、単一障害点になることに留意すること。
・クラウドサービスは、運用していくなかで、様々な構成や設定を見直す可能性があり、管理事項も多く、セキュリティホールが発生する可能性がある。対策として CASB（Cloud access security broker）などを用いて、自動的に設定や複数のクラウドサービスにおける管理上の問題を一元的に検知、解消する仕組みを導入すること。
・クラウドサービスにより提供される仮想マシン、データベースや AI 開発等各種サービスは、他のクラウドサービスへも移行しやすいように、相互運用性が高い状態で利用すること。
・IP ファイヤーウォール等を活用して、海外のサーバーを利用しないように構成すること。
・クラウドサービスとデータセンターを接続するネットワークやネットワーク接続に関連するサーバー、必要に応じてネットワーク監視を行うための接続サービスを選定する際には、ベンダーロックインにならないように、複数の接続サービスを、性能、費用面、可用性、柔軟性について比較検討し、最適なものを選定すること。
・サービスレベルが高い機能に関しては、クラウドにおけるリージョン及び、データセンター内のオンプレミス環境にも冗長化を行うこと。
・クラウドやデータセンター内のネットワーク構成については、自動的に構成や接続状況を確認できるようにし、アップデートの更新管理の負担がないようにすること。
・データセンターやクラウドの構成について自動的に管理し、アップデーターの適用状況を監視し、配布・更新を簡便にできる方法を導入すること。
・データセンターの選定にあたっては、PUE（Power Usage Effectiveness）に配慮して選定すること。

（２）コンテナ技術の利用に関する遵守事項

・コンテナを活用する場合は、コンテナの可用性に十分配慮し、冗長化するとともに、複数のコンテナを連携して利用する場合は、コンテナの一部が停止しても、即時に同等の機能を有するコンテナが起動し、連携を阻害しないようにコンテナオーケストレーションを構成すること。
・コンテナ技術を活用するにあたっては、処理速度や機能維持を考慮して、マイクロサービスによる設計を行うこと。その際に、特定のコンテナやネットワーク機器に負荷がかからないように、負荷分散や負荷の回避経路を自動的に構成できるように設計すること。

（３）外部サービスの利用に関する遵守事項

・パイプラインや各種データ、資料の共有に関して、外部サービス（SaaS 等）を利用する場合は、サプライチェーンリスクに配慮して、他国のサーバーを利用しないように設定すること。また、外部サービスとの通信は、TLS1.2 レベルの暗号化すること。ただし、特定の回線事業者や開発企業が提供するネットワークサービスではなく、オープン技術によりネットワーク接続すること。

・外部サービス（SaaS 等）を利用する場合は、ISMAP（政府情報システムのためのセキュリティ評価制度）へ登録されているサービスを利用することが望ましい。もしくは、HIPPA 等医療情報管理に関する基準の適用をしているサービスを利用することが望ましい。

（４）解析環境等の利用に関する遵守事項

・解析者への解析環境の提供は、クラウド上へ解析者が TLS1.2 で暗号化された VPN や IAP（Identity-Aware Proxy）を利用して接続することとし、個別にデータのみの提供は行わない。また、解析環境への接続は、Web により利用申し込みを行うとともに、申し込みが承認された際には、人的に提供する環境ではなく、自動的に必要な GPU やストレージサイズが構成される仕組みを構築すること。

・解析環境へのアクセスは、プライベートの電子証明書により認証・認可を行うこと。また、関連するサービスへのアクセスは、一つの認証・認可により必要なデータへの認証・認可が行えるようにすること。また、端末認証にあたっては、多要素認証を行うこと。

・解析者が利用する端末については、一定程度のセキュリティリスクを低減するための要件を求める必要がある。統一基準群のガイドライン等を参照し、当該端末要件について取りまとめて専門委員会の承認を得るとともに、利用者に提示すること。

・変異の検出や各種自然言語処理に AI を活用する場合、AI の質（AUC や教師データを使用している場合は、アノテーションの質や学習の最適化など）や採用されているアルゴリズム、知財に関する問題の有無を評価し、導入すること。また、常に、最適な AI の維持が可能であるように、AI 維持開発基盤を保有すること。

（５）システム監視やセキュリティ対策に関する遵守事項

・システム監視を行うにあたって、クラウドやオンプレミス、スパコン、セキュリティ等の構成要素毎に個別に監視するのではなく、可能な限り、監視に用いるダッシュボードは、一元化すること。

・本事業において環境を整備・構築する事業者と、当該環境の運用及びセキュリティ監視を行う事業者が異なる場合も想定し、開発事業者の特定技術に依存せず、セキュリティ監視要員を確保しやすい汎用的な監視環境を整備すること。

・外部とのデータをやり取りする場合は、データの無効化ではなく、無害化を行い、マルウェアの混入を回避すること。

・セキュリティ監視や検知は、ネットワーク機器及びクラウドに関してもログだけではなく、ペイロードを監視・検知できるようにすること。

・セキュリティ監視に用いるリスク判定や脅威インテリジェンスについては、その方法や質などの情報を公表しているものから、比較検討し、最適なものを採用すること。また、随時最適化するために、見直すこと。
・ネットワークの出口対策においても、不正接続が発生した際に接続先の通信のみ、即時自動遮断できるようにすること。
・システム構築後や更改後は、脆弱性診断はもちろんのこと、専門的なペネトレーションテストを行うこと。その際に、特定の領域だけではなく、アプリケーションから基盤、データへのアクセスまで、全体をテストすることを前提にペネトレーションテスト計画を策定し、実施すること。
・以上のセキュリティ運用監視計画を策定のうえ、厚生労働省や専門委員会の承認を得ること。

３．構築事業の管理に関する留意事項

・データセンター構築にあたっては、プロジェクト管理を徹底し、作業工数や WBS(Work Breakdown Structure)、ガントチャート、WBS ディクショナリ、工程毎のコストを基準計画として明らかにすること。
・プロジェクト管理者は、EVM（Earned Value Management）を用いて、プロジェクト開始時に、関係者による作業内容を承認してから作業を開始すること。また、プロジェクト管理者は、工程の作業が完了した際には、WBS ディクショナリに記載される完了基準を満たしているか確認するとともに、定期的に EVM 値等、構築作業における成果の状況について、厚生労働省と専門委員会に報告すること。厚生労働省や専門委員会は、進捗が大きく遅延するなどの課題がある場合は、是正要求を行うこと。
・構築作業において、要件定義、構築、テスト、移行等、フェーズの配分に関して、プロジェクト開始時に、科学的な見積もりを行い、工程配分の妥当性を確認すること。

４．共通事項

・構成技術の採用にあたっては、各構成について、同様の技術を複数比較検討し、合理的な理由により最適な技術を採用すること。
・データセンターの技術構成や採用技術の妥当性については、厚生労働省や専門委員会にて承認を得ること。
・一定の更改期間を設けることなく、最適かつ最新の技術を随時導入可能であるように構成すること。