テクニカルノート

Illumina Connected Analyticsによるセキュリティ、プライバシーおよびコンプライアンス

データのプライバシーと保護に関する高い基準に合致

- サイバーセキュリティを保証するためのイルミナによる措置とカスタマーの責務
- Illumina Connected Analytics（ICA）インフラストラクチャーが実施するセキュリティ対策
- グローバルなデータ保護およびプライバシーに関する基準と認証に準拠
- グローバルなデータ保護およびプライバシーに関する法律と規則の順守

illumina®

はじめに

次世代シーケンサー(NGS)テクノロジーの進歩によりデータ生成量が劇的に増加し、データ解析と解釈に課題を生み出しています。Illumina Connected Analytics(ICA)は、インフォマティクスの運用と科学的洞察を推し進める、セキュアなゲノムデータプラットフォームです。ICAは、豊富なRESTfulアプリケーションプログラムインターフェース(API)およびコマンドラインインターフェース(CLI)ツールを備え、拡張性のあるプラットフォームを提供し、ワークフローの効率を最大にします。このプラットフォームは、地域および世界の適用される規則や基準の要件に従って開発されました。高機能なゲノムデータプラットフォームと第三者の検証済みセキュリティを組み合わせることで、ICAは患者由来のゲノムデータなど、機密性の高い情報を扱うお客様の厳しいセキュリティ要件を満たすことができます。本文書は、ICAがセキュリティ要件および適用されるデータ保護の法律と規則に従ってどのように開発されたかについて詳述します。

ICAのセキュリティ対策

機密性の高いヒトゲノムデータの高レベルな保護を確保するために、幅広いセキュリティ対策が実施されています。ICAはデータセキュリティを提供し、法規制の順守を念頭に設計され、ISO 27001およびISO 13485などの国際基準に準拠します。公共施設と企業両方のきめ細かいアクセスを制御して、クラウド上での処理、インターネットを介した転送、または静止状態での保存など、プラットフォーム全体にわたるデータフローの完全性を保証します。ICAは、機密性の高い患者情報を格納するため多層的なデータセキュリティを備えています(表1)。

ICAはセキュアなクラウド環境上に配置され、最高水準の隔離性を確保しています(図1)。解析パイプラインはコンテナ内で実行され、プラットフォームごとに設定した境界内に留まります。これにはデータへのアクセスおよびリソース消費が含まれます。これによりICAは性能を損ねることなく、堅牢なプラットフォームとインフラストラクチャーのセキュリティを提供できます。

包括的なプラットフォームセキュリティアーキテクチャー

ICAは、臨床、製薬または研究領域における個人または企業に対して、高性能かつ拡張性の高いデータ処理とストレージ要領をサポートします。イルミナのシーケンス装置とのセキュアでシームレスな統合により、ICAへの効率的なデータ取り込みが可能になります。セキュリティ対策により転送中および保管中のデータを保護します。

転送中のデータ

ICAはウェブベースのAPIを介して装置と通信します。シーケンス装置とICAとの間のすべてのトラフィックは、機密性の高い情報がインターネットを通過する際にこれらの情報を暗号化するインターネット標準である、トランスポートレイヤーセキュリティ(TLS 1.2)を使用します。すべてのサービスメソッドはAPIキーシグネチャーを必要とし、その他すべてに対するサービスは拒否されます。リクエストは不正使用されていないか監視されます。

保管中の暗号化

ICA内のお客様のデータは保管中、Advanced Encryption Standard (AES)-256を使用して暗号化されています。

ネットワーク脆弱性の回避

境界線コントロールは、ネットワークの外部境界線および主要な内部境界線での通信をモニターし、規制します。これらの境界線コントロールはルールセット、アクセスコントロールリストと設定を用いて、特定の情報システムサービスに情報の流れを強制的に制御します。アクセスコントロールリスト、すなわちトラフィックフローポリシーはトラフィックの流れを制御するためにそれぞれ管理されたインターフェース上に設置されます。

その他のコントロール:

- 第三者のセキュリティ会社による定期的なペネトレーションテスト
- 定期的なネットワークスキャン
- データ送信のための電子メールの使用に対するポリシー。マルウェアを含む可能性のある添付ファイルからのリスクを低減
- 既知の固定イメージとして展開されるシステムホスト(バーチャルインスタンス)
- Open Web Application Security Project (OWASP)ガイダンスに準拠した自動的セキュアコードスキャン
- ネットワークおよびホストベースの検出と予防的セキュリティコントロール

表1：ICAデータセキュリティレベル

セキュリティ管理	ICAの機能	利点
ログインポリシー	パスワード要件および非活動時のタイムアウト期間を管理者が管理	高水準の機密性を保証
オブジェクトオーナーシップ	初期設定では、いずれのオブジェクト[a]もそのプラットフォームに当該オブジェクトを初めに導入したユーザーが所有 オブジェクト[a]の所有者は、オーナー権限を介して、その他のユーザー、企業およびコミュニティー別にそのオブジェクトへのきめ細かいアクセスを管理	きめ細かいアクセス権限を保証
監査ログ	プラットフォーム内のオブジェクトに関する行動を記録	法規制の順守を念頭において設計
役割ベースのアクセス	包括的なマトリクスにより、クライアントの管理者が組織の要件に適合させるためにきめ細かいセキュリティ定義を設定。きめ細かいセキュリティ管理を厳密に制御でき、誰がそのプラットフォーム内で何をできるかについて、すべてのオブジェクト[b]に適用可能	管理者が組織の管理要件を実行可能
公開鍵暗号基盤（PKI）	デジタル証明、公開鍵暗号および承認機関を企業規模のネットワークセキュリティアーキテクチャーに統合。このフレームワークにより、公開鍵暗号の生成、プロダクション、配布、管理、会計および破壊が可能	電子署名および暗号化能力を提供 プラットフォーム全体にわたるデータ[b]フローの完全性を確保
データ暗号化	すべてのデータは、転送中（TLS）および保管中（AES 256/128）に暗号化。 データダウンロードおよびパイプラインに対するインプットとしてのデータ使用を含むあらゆる行為が実施される前に、データの完全性を検証。 データ漏洩の発生時には、ICAセキュリティ担当者が警告を受け取り、データは隔離。根本原因が特定された後、適切な措置を実行	転送されたデータを隠し、権限のない当事者に理解不能とすることで、個人データの機密性を達成するために使用
2要素認証[c]	機密性の高い行為に対する認証ステップ[a]	高いセキュリティレベルによってアカウントアクセスを確保

a. 機密性の高い行為には、パイプラインの変更、アップロード、データ設定が含まれます
b. データはデータセットとパイプラインとして定義されます。オブジェクトはデータベース内のあらゆる記録として定義されます
c. Enterpriseのお客様のみ利用できます

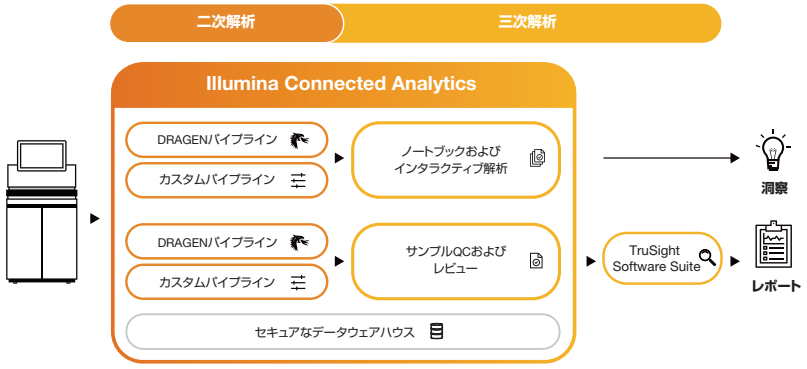

図1: ICAは単一のサンプルおよび集団レベルのワークフローに対応します

主な性能

1. ワークフロー内での透明かつ効率的なデータアップロードと処理を実現する、シーケンス装置とインフラとのシームレスかつセキュアな統合。

2. バージョン制御されたデータ解析を実行する、設定のしやすい、柔軟性と拡張性のあるパイプライン。

3. パイプラインの並行処理によるオンデマンドのスケーラブルなデータ解析で、必要な時のアクセス集中に対応。

処理時間、待ち時間または効率性を損なうことなく、解析パイプライン性能はストリーミングおよび大量データセットのバッチ処理に対応します。大量データは、関連する規制要件すべてを順守し、セキュアかつ暗号化された形でプラットフォーム内において処理されます。

グローバルなデータセンターの配置

グローバルな配置モデルにより、ICAはデータソースに近い場所でデータを保存し、コンピューティング解析を実施でき、地域ごとに、適用されるデータ保護法と規制要件に順守してデータ保管することができます（図2）。これにより、お客様は新しいプロジェクトを開始する際に特定の場所を選択できるようになります。プラットフォームの戦略的かつ世界的な展開により、現在世界中でサポートされている場所のうちの1カ所でデータを処理し、保存できます。

データレジデンシーコントロール機能により、ユーザーは世界中のプロジェクトとデータ処理を単一のインターフェースで管理できます。データレジデンシーは、複数のデータセンターを別々に管理する負担なく、セキュアなコラボレーションとデータ共有を可能にします。

堅牢なデータ可用性とコントロール

ICAでは、高いレベルのデータ可用性を保証する信頼性の高いデータセンターパートナーを厳選しています。さらに、イルミナは、これらのデータセンター内でICAが高水準のセキュリティ要件に従って動作できることを積極的に保証しています（表2）。

可用性

内部および外部の可用性リスクを軽減するために、ICAには事業継続性と災害復旧計画が組み込まれています。ICAは、Uptime Instituteが作成したTier III基準に準拠したISO/IEC 27001:2013認証施設での高可用性クラウドインフラ上にインストールされています。

データのセキュリティおよび冗長性は、専用のフェイルオーバーアプリケーションによって保護されています。このアプリケーションは2カ所のデータセンターに分散されたアクティブ/パッシブセットアップとして確立された中央プラットフォームに依存しています。障害発生時、この中央プラットフォームはバックアップノードに転送されます。そのようなフェイルオーバーに対する目標復旧時間（RTO）は6時間ですが、目標復旧ポイント（RPO）はゼロであり、バックアップデータベースに対してプロダクションデータベースを同時に方向付けることによって直ちに達成されます。

完全性

ICAは公開鍵基盤（PKI）を実施することでデータ完全性を確保します。このPKIはクラウドベースのプラットフォーム内であらゆる行為が実施される前にデータ完全性を検証するよう設計されています。

機密性

ICAはクラウド環境中のデータ処理活動の機密保持を最優先するため、「転送中」（TLS 1.2）および「保管中」（AES-256/128）両方のデータの仮名化と暗号化をしています。

データ暗号化に加え、ICAは必要なアクセス制限を実行し、プラットフォームへの不正なアクセスを制限します。このことは、強力な認証機構を使用した識別とアクセス管理によって機密性をさらに確保するために役立ちます。また、処理を行う従業員と契約者が守秘義務によって拘束されることも示唆します。*

* 特定の情報については、一部の管理者はいわゆる「ゼロ知識」ソリューションを検討する可能性があります。「ゼロ知識」ソリューションでは、クラウドサービスプロバイダーは暗号化キーにアクセスできないため、ホストされた情報の暗号解読のアクセスはできません。これにより機密保持リスクは大幅に低下しますが、「ゼロ知識」ソリューションの使用は強制ではありません。追加の契約上および組織的な予防手段など、機密性を確保するために代わりの対策を実施する場合もあります。

図2：AWSの地域データセンター上にあるICAのグローバルな配置

表2：ICAデータセキュリティ要件

セキュリティ要件	ICAの機能	利点
可用性	信頼できるデータセンターとの連携	専用のネットワーク接続性、冗長性、連続電力供給（UPS）および効果的なデータバックアップ戦略を保証
完全性	PKIインフラストラクチャー	プラットフォーム全体にわたるデータフローのオリジナリティーと完全性を確保
機密性	「転送中」（TLS 1.2）および「保管中」（AES 256/128）のデータ暗号化	データ機密性を確保
透明性	顧客特異的なデータレジデンシー要件に順守	データセンターの場所を開示
データ分離	業界標準のデータ分離技術	データが誤って第三者と共有または第三者によって開示されないことを保証
携行性	データ出力に対する標準化されたツール	ベンダーロックインなくクライアントデータをエクスポート
アカウンタビリティー	ITアカウンタビリティーを確保するためのメカニズム	常にすべての行為を記録

透明性

ICAはほとんどのデータレジデンシーとプライバシー要件に順守します。データセンターの地域とプロバイダーは開示されます。

分離

ICAは、技術的および組織的手段（きめ細かいセキュリティコントロールによる役割ベースのアクセスなど）を介して、Need-to-Knowの原則を含む業界標準のデータ分離技術を実行することで、最も高性能なデータ分離を提供します。

移植性およびイグジットマネジメント

ICAで処理されるデータは常にお客様が利用できる状態になっています。データ出力用の標準的なツールを使用することで、お客様が別のクラウドサービスプロバイダーに移行したり、相互運用性の欠如によりサービスを請け負ったりできないベンダーロックインのリスクはありません。

記録保管および監査ログ

ICAでは記録保管と監査ログが可能で、1つのオブジェクトの閲覧を含め、すべてのオブジェクト、アクションおよびアクティビティーに対して常にプラットフォーム内でのITアカウンタビリティーを確保します。

イルミナのセキュリティプラクティス

イルミナのサイバーセキュリティプログラムは、経営幹部のリーダーシップによって推進されています。イルミナの取締役会および上層部経営陣は、サイバーセキュリティプログラムの詳細とロードマップを年4回以上アップデートし、適用される法律および規則に順守して規制項目および事業目標を達成するための能力と投資の適切な配分を確保しています。サイバーセキュリティプログラムは社内チームおよび独立した第三者によって毎年見直され、米国立標準技術研究所（NIST）サイバーセキュリティフレームワークへの順守を評価しています。イルミナは優れたサイバーセキュリティ専門家の雇用と育成に力を注いでいます。現在のサイバーセキュリティチームのメンバー全員が1つ以上のサイバーセキュリティ認証を保持しており、チーム内の幅広い専門性を確保しています。

製品設計中のリスク管理

ICAおよびイルミナ製品開発には、脆弱性を最小限に抑えるためのセキュリティ設計要件が組み込まれています。例えば、イルミナの製品オペレーティングシステムは、データセキュリティを損なうことなく、攻撃対象領域を減らし当該機器の機能に適したユーザーアクセスレベルを実現しています。

クラウドベースの製品について、イルミナはプライバシーバイデザインに注力しており、これにより個人データの処理に関与する新製品、プロセス、またはサービスの開発ライフサイクルにおける早期の段階で、プライバシーコントロールを組み込み、プライバシーリスクへの対処が可能となります。

イルミナはセキュアな設計とアーキテクチャーのレビュー、リスク評価、セキュリティ上の欠陥に対するソフトウェアの検証および脆弱性に対するモニタリングを実施しています。これらは、イルミナのセキュアな開発ライフサイクルの重要かつ現在進行中の活動の一部です。

リスク解析およびセキュリティ検証

イルミナは産業パートナー、お客様およびサポートチームと連携して、サイバーセキュリティリスク環境と装置インストールベースの配置を継続的に評価しています。新製品は高い基準に対応するように設計されており、進化するサイバーセキュリティリスクと脅威に対応するために最新の企業規模のサイバーセキュリティプラクティスが実行されています。

イルミナはクラウドソフトウェア製品に対して、ソフトウェアコードのセキュリティ検証を日常的に実施しています。標準的な構築プロセスの一環として、ソフトウェアコードは定期的にセキュリティ欠陥に対する静的解析を受けています。内部および外部のペネトレーションテストの専門家たちが、年1回、セキュアな開発ライフサイクルの主要な構成要素として、既存のクラウドソフトウェア製品を検証しています。

イルミナ従業員のセキュリティプラクティス

世界中のイルミナの採用候補者を対象に、バックグラウンドチェックが実施されています。このバックグラウンドチェックには、学歴、大学の学位、前職および犯罪歴が含まれます。ポリシーと手順に関する文書では、セキュリティ違反行為の防止、検出、抑制および関連時のガイドを記載しています。

セキュリティ認識とトレーニングプログラムでは、ICAをサポートする従業員にイルミナのセキュリティポリシーを伝えています。自動化されたコンプライアンスモニタリングシステムが従業員のトレーニング要件の順守を追跡します。ICAをサポートするイルミナの全従業員は、イルミナセキュリティポリシーの不順守についての懲戒処分を承知しています。

- ICAをサポートするイルミナの全従業員は、お客様のデータの適切な取り扱いに関して毎年トレーニングを受けます。
- お客様のデータのダウンロードは制限されます。
- イルミナの従業員は、最小権限の原則、すなわち従業員が自身の職務を遂行するために最小限のアクセスレベルのみ許可されているという原則に従い、必要に応じてICAへのアクセスが許可されています。
- イルミナは従業員の許可に関して定期的に計画されたレビューを実施し、必要に応じてアクセスレベルを更新します。
- システムへのアクセスは記録され、自動化されたチケットシステムに文書化されます。
- 従業員がイルミナを離職する際は、製品環境、イルミナアプリケーションおよびITシステムへのアクセスは取り消されます。イルミナが所有するすべての機器とバッジも返却されます。

ICA認証

ICAは、適用されるデータ保護、セキュリティおよび品質要件を順守する必要のある、規制環境で活動するお客様をサポートします。ITはアマゾンウェブサービス（AWS）によって提供される既存のクラウドインフラ上に構築されているため、いくつかのAWS標準と認定を共有しています（表3）。さらに、ICAはさまざまな国際的に認められた、ISO 27001やISO 13485などの基準にも準拠しています（表3）。データセキュリティ認証の包括的範囲を提供することで、ICAはお客様の管理上および経済的負担を緩和します。

ISO 27001

ICAは、大量のオミクスデータおよび健康データを処理するためのクラウドベース解析プラットフォームの開発、管理およびサポートを含むすべての行動範囲に対して、独立監査人からISO 27001認証を取得しています。イルミナはISO 27001の要件に準拠する情報セキュリティマネジメントシステム（ISMS）を運用し、維持しています。

情報セキュリティ管理

- セキュリティ認識およびトレーニング
- モニタリング
- アクセス制限およびアカウンタビリティー
- 災害復旧計画
- 認証
- 障害への応答
- 機器メンテナンス
- セキュアなメディアハンドリング
- 物理的かつ環境的なセキュリティ対策
- リスク管理
- システムとネットワークセキュリティ

ISO 13485

Illumina Connected Analytics（ICA）は、イルミナの品質管理システム（QMS）の下でのイルミナのソフトウェアライフサイクル（SLC）プロセスに従って開発されました。

イルミナは、ISO 13485要件に準拠するQMSを運用し維持しています。QMSの範囲は、遺伝子解析に用いられるジェノタイピング、遺伝子発現およびPCRの製品、機器およびソフトウェアの、設計、開発、製造、配送、設置、サービスを対象としています。さらにイルミナのQMS内のプロセスは、業界のベストプラクティスと、リスク管理についてのISO 14971やSLCについてのIE62304などの関連標準を採用しています。

表3：ICA認証と認定

認証	説明
ISO 13485	医療機器に関する国際規格で、QMSに対する要件を規定。組織は、お客様および適用される規制要件を常に満たす医療機器と関連サービスを提供する能力があることを証明する必要がある
ISO 27001	情報セキュリティに関するリスクを管理する国際規格。ISO 27001への認証は情報管理を証明。この規格はISMSの確立、実施、運用、モニタリング、維持、継続的な改善を目的としたプロセスベースのアプローチを採用
AWS規格と認定	
Service Organization Control 1/SSAE 16/ISAE 3402	お客様のデータを保護するためにAWS管理が適切に作成され、個別管理が効率的に機能していることを検証する監査
連邦情報セキュリティマネジメント法（FISMA）中位レベル	連邦情報システムセキュリティを強固にするために米国政府によって許可された認証評価。参考として、NIHデータセンターはFISMA中位レベル（Moderate）と評価
Payment Card Industry Data Security Standard Level 1	電子決済セキュリティを高めるための標準設定。AWSは最高レベルと評価
連邦情報処理規格文書140-2	暗号作成モジュールに対応する要件を指定する米国政府のコンピューターセキュリティ規格

ICAの法律および規則状況

イルミナは適用されるデータ保護およびセキュリティ規則と要件への準拠に注力しています。ICAはセキュリティガイドラインを特徴とし、その運用の機密性、完全性および可用性を維持し、法律および規則の要件を満たすために制御します（表4）。

CLIAおよびCAP

ヒト検体のシーケンスを実施する米国のお客様は、1988年のClinical Laboratory Improvement Amendments（CLIA）で説明されているように、Centers for Medicare and Medicaid Services（CMS）[1]の権限の下にあります。[2] CLIA規制は、診断、予防および疾患の治療、または健康評価のためにヒト検体に実施する臨床検査に対する品質基準を制定しています。

CLIA規制は検査結果の正確度、信頼性および適時性を確保するために策定されています。規制には、検査能力、検査管理、品質管理、担当者の適格性評価および品質保証に対する品質基準が含まれます。

臨床検査室は、米国臨床病理医協会（CAP）によって制定されたより厳しい基準の下で評価されることを選択できます。[3] 規制上の観点から、CAP基準はCLIA規則に必要とされる以上の基準として認識されています。そのため、CAPによる認定は、同様にCLIA規則への準拠も認定するとCMSによって公式に見なされます。

CLIAおよびCAPに対するICAのサポート

CLIAおよびCAPに適合する検査室はICAを用いてデータを保存、管理および解析できます。ICAは検査室がデータ完全性、精度および信頼性に対処できるさまざまな主要な機能を提供します：

- シーケンス装置からアップロードされたデータをチェックし、ソースデータとの整合性を確認します。
- ICAツールとパイプラインはバージョン管理されています。修正を防ぐための手順を整備しています。
- 結果の解釈を変える可能性がある機能はバージョン管理されます。新たなバリデーションが完了するまで既存のバージョンが使用されます。
- 詳細なログが、実施したすべての解析を説明します。

GDPR

ICAは、GDPRの基盤として使用されるプライバシー原則に従うように構築されています。イルミナは、製品の設計と構造に技術的および組織的対策を実行することで、お客様が個人データ、具体的にはICAで処理されるゲノムデータという特殊な個人データを保護できるよう支援します。

ICAのそれぞれの主要なリリースは内部プライバシー評価の対象であり、あらゆる同定されたプライバシーリスクを同定し、適切に緩和します。さらに、イルミナは各当事者のGDPR義務を満たすために、お客様およびサブプロセッサーと契約条項を締結します。

HIPAA

ICAはHIPAA要件に準拠するように設計されており、これにはセキュリティに関するルールとプライバシーに関するルールを満たすために必要な業務管理および技術管理の実行が含まれます（表5）。

また、イルミナは各当事者のHIPAA義務を満たすために、お客様（すなわち、対象事業者）および契約者と契約条項を締結します。

PIPEDA

カナダでは、個人情報の保護はPersonal Information Protection and Electronic Documents Act（PIPEDA）によって規制されています。イルミナはISO 27001認証に対して実施されるポリシーおよび手順を適用しており、これにはPIPEDAガイドラインにも含まれる管理を含みます。Office of the Privacy Commissioner of Canada（OPC）は、リスク管理、セキュリティポリシー、人的資源のセキュリティ、記録管理、アクセス制限、技術的セキュリティ、物理的セキュリティなどを含むPIPEDAの合理的な予防措置への準拠を監視しています。

その他のデータプライバシーに関する法律および規則

欧州および北米のプライバシー法に対応することで、ICAはイルミナのお客様のほとんどのデータ保護義務に対処していますが、その他のプライバシーに関する法律および規則の出現および発展に伴い、これらの法律の下で順守義務のあるお客様を支援するように設計された機能を取り込むために、イルミナはICAを継続的に更新します。

表4：ICA規制要件

規制/要件	説明
CLIA、米国	診断、予防、疾患治療または健康評価のためのヒト検体に実施する臨床検査に対する品質基準を策定した規則
CAP	CLIA規則に必要とされる以上の厳格な基準として認識されている
GDPR、EU	欧州連合（EU）および欧州経済領域（EEA）内のすべての個人を対象としたデータ保護とプライバシーに関するEU規則
HIPAA、米国	米国における保護された健康情報（患者データ）を処理する企業および事業協力者を対象に規定された法律
PIPEDA、カナダ	商業活動における組織による個人情報の収集、使用、開示を規定したカナダの連邦法
DSPTK、英国	健康データに適用できる2018年データ保護法に基づくデータ保護の法律および英国でのGDPRの補完を含む、情報ガバナンス基準

DSPTK

Data Security and Protection Toolkit（DSPTK）は英国National Health Service （NHS）が開始し、National Data Guardianの10のデータセキュリティ基準とGDPRの関連要素に対する組織の実績を測定し、公表するオンラインの自己評価ツールとして役立ちます。また、DSPTKはCyber Essentials PlusやISO 27001を含むその他の認証されたデータセキュリティのベストプラクティスにも対応します。ICAは、英国における健康データに適用できる2018年データ保護法に基づくデータ保護に関する法律を含むDSPTK基準の現行バージョンの義務を満たします。

お客様のセキュリティ管理

ICAの使用はさまざまな責務をお客様の管理下に置いており、このことはAWSの責任共有モデルに準拠します。お客様は、Software as a service（SaaS）ソリューションの使用を考慮したリスク評価を実施し、リスク評価の結果は各お客様へのプライバシーおよびセキュリティ管理の見直しに反映する必要があります。例えば、パスワードポリシーはICAアカウントおよびパスワードの共有を禁止していなければなりません。施設はアクセス承認のためのプロセスと手順を確立し、すべてのユーザーに許可されているアクセスに関する定期的なレビューを実施しなければなりません。

表5：ICAにおけるHIPAAセキュリティ規則管理

セキュリティ管理	説明
業務管理	• セキュリティ違反を防止、検出、抑制、修正するためのポリシーおよび手順 • セキュリティ担当者はセキュリティポリシーおよび管理を策定し実施する責務がある • お客様のデータにアクセスする従業員は適切かつ承認されていることを保証する手順 • お客様のデータへのアクセスを許可するためのプロセス • セキュリティポリシーについてトレーニングされた従業員 • 障害発生報告のためのプロセス • データのセキュリティに影響を及ぼす環境上および運用上の変更の定期的な評価 • ユーザーデータを取り扱うすべての新機能に対して実施されるプライバシー影響評価（PIA）
物理的な管理	• 施設アクセス制限の実施 • セキュアなデータセンターにおけるICAのホスティング • ワークステーションセキュリティに関するポリシー • モバイル機器に対するポリシーおよび手順 • ICAをサポートする機器の一覧を維持
技術的な管理	• 各ユーザーに対する固有のユーザーID • ICAまたはお客様の組織の識別管理システムによるユーザー認証 • 転送中のデータの完全性を保護 • トランスポートレイヤーセキュリティをベースとした転送中の暗号化 • ユーザー起動のデータ削除性能
ISO 27001による管理	• A.5 情報セキュリティのためのポリシー • A.6 情報セキュリティに関する組織 • A.7 人的資源のセキュリティ • A.8 資産管理 • A.9 アクセス制御 • A.10 暗号 • A.11 物理的および環境的セキュリティ • A.12 運用セキュリティ • A.13 通信セキュリティ • A.14 システムの取得、開発およびメンテナンス • A.15 供給社管理 • A.16 情報セキュリティ障害発生管理 • A.17 事業継続性管理に関する情報セキュリティの側面 • A.18 コンプライアンス

さらに、お客様はICAで処理されたデータの内容を網羅するベストプラクティスを検討し確立しなければなりません。例えば、命名ポリシーは被験者情報の同定につながるものを禁止しなければなりません。ICAにアクセスするために使われるワークステーションは、アンチウイルスソフトウェア、ホストベースのファイアウォール、集中型のロギングなど、適切な保護方法をインストールする必要があります。事業継続性および災害復旧計画はICAの使用を考慮して更新されていなければなりません。

侵害通知

ICAのお客様は、侵害の一部として、データが不正アクセスされた可能性のある個人および潜在的には適切な監督当局に通知する責務があります。これには無効なログインの試み、ログオフ、ダウンロード、閲覧および共有が含まれます。このログには、日付、時間、ユーザーおよび各行為の説明が含まれます。データ修正の記述は、データを修正するために使用したツール、すなわちAPIコールの名称を含みます。APIにより、ユーザーは外部システムで監査ログを管理することが可能です。

まとめ

ICAは、次世代シーケンサー（NGS）テクノロジーにおける継続的な進歩から生じる大量のデータを管理、解析、解釈するために構築されています。研究、臨床治療、ヒトの診断のための大規模なゲノムデータの保存と共有は、ローカルおよび世界的な基準と共に包括的なデータセキュリティと法規制の順守を必要とします。ICAは、これらのニーズを満たし、適用できるデータセキュリティとプライバシー要件に準拠しつつ、大量のゲノムデータの迅速かつ効率的で経済的な処理方法を提供するために開発されました。

詳細はこちら

jp.illumina.com/ConnectedAnalyticsをご覧ください。

参考文献

1. Centers for Medicate and Medicaid Services. www.cms.gov. Accessed August 18, 2021.
2. Clinical Laboratory Improvement Amendments (CLIA). www.cms.gov/regulations-and-guidance/legislation/clia. Accessed August 18, 2021.
3. CAP Guidelines. www.cap.org/protocols-and-guidelines/current-cap-guidelines. Accessed August 18, 2021.

イルミナ株式会社

〒108-0014 東京都港区芝 5-36-7 三田ベルジュビル 22 階
Tel (03) 4578-2800 Fax (03) 4578-2810
jp.illumina.com
www.facebook.com/illuminakk

販売店

Pub. No. M-GL-00333 v2.0-JPN 30AUG2022