illumina®

BaseSpace® Sequence Hub のセキュリティーおよびプライバシー

さまざまなセキュリティー機能でゲノムデータを保護

はじめに

BaseSpace Sequence Hub はゲノムデータマネジメントおよび解析用の SaaS 型サービスです。顧客データの機密性の保護、統合性、利便性に重点を置いています。包括的なポリシー、プロセス、セキュリティーおよびプライバシーのコントロールをセットで揃えています。

BaseSpace Sequence Hub は単一インスタンス、マルチテナント展開として実装されます。隔月のアップデートはトランスペアレントで、ユーザー側のアクションを必要としません。おもなアップグレードは 2 週間前までに、リリースノートにて伝達されます。

BaseSpace Sequence Hub はソフトウェア開発ライフサイクル（SDLC）にて、ビジネスニーズと顧客インプットに基づき、特徴、コンテンツ、機能性、バグ修正の優先度を決定。最新のアジャイルソフトウェア開発を使用して、設計およびユニットテストが行われます。サービスアップデートは比較的小規模かつ高頻度で行われ、お客様に影響を与えるリスクを低くしています。変更時の検証では、自動回帰テストと手動テストが、ステージ / 生産環境から分離された試験環境にて行われます。

プラットフォームセキュリティーの取り組みとして、試行済みのアプローチ Amazon Web Services（AWS）[1] が、内部テスト手順と組み合わされています。また、これらの手段を採用することで、組織化された多くの IT インフラストラクチャーによってセキュリティーニーズを満たしたクラウドゲノムソリューションが提供されます。このテクニカルノートでは、BaseSpace Sequence Hub の基本セキュリティーの特徴を説明しています。これらのセキュリティー機能により、お客様の規制や規格（HIPAA/ 医療保険の携行性と責任に関する法律など）の遵守をサポートします。

BaseSpace Sequence Hub のセキュリティープラクティス

BaseSpace Sequence Hub はラン実行中のシーケンサーから直接データをインポートするため、お客様はランの完了後すぐにデータ解析を開始できます。シーケンス装置、データ解析、ストレージサーバー間の通信中、複数のセキュリティー手段にて、トランジット中のデータを保護します。

ユーザーはローカルと BaseSpace Sequence Hub（MiniSeq® System を除く）の両方でデータを保存できます。イルミナのシーケンスプラットフォーム（MiniSeq、MiSeq®、NextSeq®、HiSeq®）は、トランジット中の暗号化と、ラン実行中に生成されたデータの検証をサポートします。ブローカーソフトウェアとアプリケーションプログラムインターフェースによる相互作用で、ネットワーク中断、レイテンシー、不完全なトランスミッションの補足およびリキューが自動的に行われます。

ユーザーはランセットアップ中に、BaseSpace Sequence Hub へのデータ送信決定を開始できます。このオプションを選択すると、ランは認証されユーザーアカウントが追跡されます。Base Space Sequence Hub Enterprise でも、セキュリティーアサーションマークアップランゲージ（SAML）2.0 規格を採用した、第三者認証によるシングルサインオンがサポートされます。

ユーザーは BaseSpace Sequence Hub[2] へのアップロード時に、個人を認識できる直接的な情報（氏名、誕生日など）をすべてゲノム情報から削除することを求められます。これは、各サンプルのアップロード前に、バーコードなどのユニークなコードやサンプル識別子を付与することによって実行できます。BaseSpace Sequence Hub を使用するお客様は、直接的な識別子情報をすべて、BaseSpace Sequence Hub 外にある別の暗号システムにて保存することが推奨されます。

トランジット中のセキュリティー

BaseSpace Sequence Hubは、ウェブベースのアプリケーションプログラムインターフェースを通じて装置と通信します。シーケンサーおよび BaseSpace Sequence Hub 間のすべてのトラフィックで、トランスポートレイヤーセキュリティー（TLS）が使用されています。TLS はセキュリティーが求められるインターネット上の通信において、暗号化を行うプロトコルです。すべてのサービス手段において、アプリケーションプログラムインターフェースの署名鍵が求められ、署名者以外に対するサービスは拒絶されます。不正防止のため、リクエストがモニタされます。

BaseSpace Sequence Hub へのアクセス

BaseSpace Sequence Hub へのアクセスは、ウェブポータルからログインします。ユーザーは BaseSpace Sequence Hub 認証で、企業のお客様のユーザーはシングルサインオンでも認証を行えます。BaseSpace Sequence Hub Enterprise のお客様はパスワード長および複雑性のポリシーを決定し、パスワードの不正使用防止のため、アカウントロックアウトおよびロックアウト期間を設定できます。

無効なログオンおよびログオフ操作はシステムに記録されます。企業のお客様のユーザーがシングルサインオンを使用する際は、ログイン活動が、お客様のシステムからもモニタされることがあります。顧客データの変更、読み込み、更新、欠失および共有も、BaseSpace Sequence Hub Enterprise のお客様のためにログ記録されます。ログ記録により疑わしいユーザー活動をモニタできます。ログ記録は .csv ファイルまたはアプリケーションプログラムインターフェースから利用できます。Virtual Private Cloud で実行されるすべてのコンピューテーションインスタンスランは、AWS クラウドに理論上独立したセクションをもたらします。このとき、バーチャルネットワーク上の AWS リソースは、イルミナによって定義されます。

データ統合性

BaseSpace Sequence Hub は AWS を通じて、顧客データを利用できる複数ゾーンに同時保存し、定期的なデータ統合性点検およびデータ損失保護のための自己回復を実行します。ですが、BaseSpace Sequence Hub は無制限のバックアップシステムではありません。削除済みのデータを取り戻せるメカニズムはありません。

安心の暗号化

BaseSpace Sequence Hub 内の顧客データは、AES-256 規格を使用して暗号化されます。

ネットワークとアプリケーションの脆弱性の回避

バウンダリーコントロールで、ネットワークの外部バウンダリおよびおもな内部バウンダリの通信をモニタおよび制御します。これらのバウンダリ制御では、ルールセット、アクセスコントロールリスト、特定の情報システムサービスに情報フローを実行する構成を採用。アクセスコントロールリストまたはトラフィックフローポリシーは、トラフィックフローを制御する各マネージドインターフェースに確立されています。

追加のコントロールには、以下が含まれます。

- 第三者セキュリティー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
- データデリバリーのための電子メール使用に対するポリシー、マルウェアを含んでいる可能性のある添付物によるリスク低減
- 重要なセキュリティー問題に対するレスポンスの優先順位づけ（プードルなど）
- 既知の固定画像として展開されたシステムホスト（バーチャルインスタンス）

ユーザーによるデータ共有

BaseSpace Sequence Hub は、協調システムとして設計されています。ユーザーは、共有できるユーザーまたは転送できるデータを制御するために、組織内部のポリシーに従う責任を負います。ユーザーは、他の登録ユーザーとの共有リクエストを送信することにより、アプリケーション内でデータを共有し、アクセス権を許可します。

ユーザーは、法的に許容される場合、技術サポートに伴うデータアクセスを一時的に共有できます。場合によっては、トラブルシューティングまたはユーザートレーニングは、スクリーン共有、または GoToAssist や WebEx などのリモートコンピューティングツールによるデータ共有をしなくても実行できることもあります。

技術サポートおよび品質コントロール（QC）

BaseSpace Sequence Hub 技術サポートチームのエキスパートには、電話か電子メールでアクセスできます。お客様とのコンタクト、お客様のイベント、レスポンスはすべて追跡させていただきます。

BaseSpace Sequence Hub は、ランの品質評価のための QC ツールを提供します。これらのツールはスタンドアロン型のソフトウェアとしても利用可能です。解析中、実行された解析内容にあわせて、ソフトウェアアプリケーションから QC ログが提供されます。

データセンターのセキュリティー

BaseSpace Sequence Hub は、AWS によって提供される既存のクラウドインフラストラクチャーに構築されています。このため、複数の AWS 規格と認定を共有しています（表 1）。AWS セキュリティーの特徴についての詳細は、Amazon ウェブサイトをご覧ください。[1]

イルミナが採用するセキュリティープラクティス

米国では、イルミナの採用候補者全員にバックグラウンド調査を実施しています。バックグラウンド調査では、教育背景、学歴、前職、犯罪歴をチェックします。従業員がセキュリティー違反を防止、発見、抑制し、相互関連づける指針となるポリシーおよび手順が、文書化および策定されています。

セキュリティー認知およびトレーニングプログラムによって、BaseSpace Sequence Hub をサポートする従業員にイルミナのセキュリティーポリシーを伝えています。自動コンプライアンスモニタリングシステムにて、トレーニング要件に対する従業員の遵守状況を追跡しています。BaseSpace Sequence Hub をサポートするイルミナの全従業員は、イルミナのセキュリティーポリシーを遵守できない状況に対して規律ある行動を取る意識を持っています。

表 1：Amazon Web Services 規格および認定

特長	詳細
Service Organization Controls 1/SSAE 16/ISAE 3402	顧客データを保護する AWS コントロールが適切に設計されていること、個々のコントロールが効果的に作動していることを確認する監査。
Federal Information Security Management Act (FISMA) Moderate	連邦情報システムセキュリティーの強化のため、合衆国政府によって与えられる認定。参考までに、NIH データセンターは FISMA moderate 評価を受けている。
Payment Card Industry Data Security Standard Level 1	増加している電子支払いのセキュリティーを定めた規格。AWS は最高レベルの評価を受けている。
ISO 27001	セキュリティーについて定めた広く知られている国際規格で、セキュリティー管理のベストプラクティスと包括的なセキュリティーコントロールについて規定。
Federal Information Processing Standard Publication 140-2	合衆国政府によるコンピューターセキュリティー規格で、暗号モジュールに対する要求事項を規定。

BaseSpace Sequence Hub をサポートするイルミナの全従業員は、顧客データの適切な取り扱いについて毎年トレーニングを受けています。顧客データのダウンロードは制限されています。イルミナの従業員は、BaseSpace Sequence Hub システムへのアクセスを必要ベースで許可されています。システムへのアクセスは、自動チケットシステムにてログ記録および文書化されています。

従業員がイルミナを退職する際は、生産環境、イルミナのアプリケーション、および IT システムへのアクセスが無効にされます。イルミナが所有するすべての設備およびバッジも返却されます。

HIPAA によるセキュリティーおよびプライバシー

BaseSpace Sequence Hub Enterprise は、HIPAA（医療保険の携行性と責任に関する法律）に準拠して設計および実装されています。アメリカ合衆国保健福祉省（HHS）は 1996 年に HIPAA を定め、[3] これを施行するため、複数の規制を設けました。なかでも HIPAA は、医療情報保護（PHI）のセキュリティーおよびプライバシーに関する国内規格を定めたものです。HIPAA でおもに定められているのは、セキュリティー規則、プライバシー規則、および違反通知規則です。HIPAA、HIPAA の歴史、個別の HIPAA 規制についての詳細は、HHS Health Information Privacy ウェブサイト [3] をご覧ください。

HIPAA の遵守

HIPAA セキュリティー規則で定められた要求事項では、保護されるべき電子医療情報（ePHI）の機密保持、統合性、および利用可能性を保証するための管理上、物理的、および技術的な保護手段が求められています。BaseSpace Sequence Hub は、HIPAA セキュリティー規則の要求事項を満たした複数の特徴とコントロールを提供します（表 2）。

お客様の責務

HIPAA 遵守を求められるお客様は、最終的に、BaseSpace Sequence Hub が内部コンプライアンスに準拠して使用されていることを保証するため、HIPAA コンプライアンスプログラムを策定する責任を負います。

イルミナはお求めに応じて、BaseSpace Sequence Hub Enterprise のお客様と Business Associate Agreement を締結します。イルミナは、BaseSpace Sequence Hub の Amazon Web Services について Business Associate Agreement を締結しています。

イルミナとの Business Associate Agreement 締結は、お客様の HIPAA 遵守サポートにつながります。BaseSpace Sequence Hub の使用を HIPAA に準拠させる適切な内部コンプライアンスプログラムを策定するため、ポリシーおよびプロセスを策定する責任を最終的に負うのは、お客様の所属する企業および団体です。

お客様が実行するセキュリティーコントロール

BaseSpace Sequence Hub を使用するため、お客様はいくつかの責任を負うことになります。SaaS 型ソリューションを使用する際は、リスク評価を考慮する必要があります。リスク評価の結果を、お客様のプライバシーおよびセキュリティーコントロールのレビューに反映させる必要があります。

お客様のポリシーをレビューし、SaaS 型ソリューションの使用を反映させる必要があります。たとえば、パスワードポリシーにて、BaseSpace Sequence Hub のアカウントとパスワードの共有を禁じる必要があります。お客様の所属する企業および団体は、アクセスを承認するプロセスおよび手順を策定し、全ユーザーに認められたアクセスを定期的にレビューする必要があります。

表 2：BaseSpace Sequence Hub のセキュリティーコントロール

セキュリティーコントロール	詳細
管理上のコントロール	セキュリティー違反を防止、発見、抑制、修正するためのポリシーおよび手順。
	セキュリティーポリシーおよびコントロールの策定および実行の責務を担うセキュリティー担当者。
	職場の従業員による顧客データへのアクセスが適切かつ承認済みであることを確認する手順。
	顧客データへのアクセスを認証するプロセス。
	セキュリティーポリシーについてトレーニング済みの職場の従業員。
	インシデントレポートの処理。
	データセキュリティーに影響を与える環境および作動変更の定期的な評価。
物理的コントロール	実装済みのファシリティーアクセスコントロール。
	安全なデータセンター内にホストがある BaseSpace Sequence Hub。
	ワークステーションのセキュリティーに関するポリシー。
	携帯端末向けのポリシーおよび手順。
	BaseSpace Sequence Hub をサポートする機器一覧の維持管理。
技術的コントロール	各ユーザーにユニークなユーザー ID。
	BaseSpace Sequence Hub によるユーザー認証、または顧客組織の ID 管理システム。
	トランジット中のデータ統合性の保護。
	トランスポートレイヤーセキュリティー（TLS）に基づいた、トランジット中の暗号。

BaseSpace Sequence Hub へのアクセスに使用するワークステーションには、ウイルス対策ソフト、ホストベースのファイアウォール、集中ログなどの適切な保護手段がインストールされていなければなりません。BaseSpace Sequence Hub の使用を考慮に入れて、事業継続および障害回復プランをアップデートする必要があります。

HIPAA に定められた違反通知

BaseSpace Sequence Hub Enterprise のお客様は、違反が生じた結果、個人情報データが損なわれる可能性のある個人に通知を行う責任を負います。監査証跡アプリケーションプログラムのインターフェースをユーザーが利用できるようになります。これには、ユーザーデータ（アクセスできる可能性のあるあらゆるタイプのファイル）へのすべてのアクセスに関する情報が含まれます。この情報には、無効なログオン操作、ログオフ操作、ダウンロード、表示、共有などが含まれます。ログには日付、時間、ユーザー、各アクションの説明が含まれます。データ変更の説明は、データ変更に使用されたツール名、またはアプリケーションプログラムのインターフェースコールで構成されています。アプリケーションプログラムのインターフェースにより、ユーザーが外部システム内にて監査ログ管理することができます。

CLIA および CAP

イルミナの多くのお客様がヒトのサンプルにシーケンスを実行します。こうした検査が実施されるラボは、メディケアおよびメディケイドサービスセンター（Centers for Medicare and Medicaid Services/CMS）[4] の管理下にあり、その旨は 1988 年の臨床検査改善修正法案（CLIA 規制）に記載されています。[5] CLIA 規制は、疾患の診断、予防、治療、または健康評価を目的にラボで実施されるヒト検体検査の品質規格を定めています。

CLIA 規制は検査結果の正確度、信頼性、適時性を保証するために設計されています。この規制では能力テスト、テストマネジメント、品質コントロール、人員適格性、品質保証の品質規格が定められています。

臨床ラボは、米国臨床病理医協会（CAP）[6] によって定められたさらに厳格な規格にて評価を受けることもできます。CAP 規格は法的観点から、CLIA 規制よりも要求事項が厳しいと認識されています。このため、CMS は CAP 認定が CLIA 規制を遵守しているものと考えています。

CLIA および / または CAP 認定と BaseSpace Sequence Hub サポート

CLIA および / または CAP 認定ラボは、シーケンスデータの保存、管理、解析に BaseSpace Sequence Hub を使用できます。BaseSpace Sequence Hub の使用には、CLIA および / または CAP 認定は求められませんが、認定がない場合、医療機関から受け取ったデータの解釈はしないでください。BaseSpace Sequence Hub のおもな特徴は、ラボがデータ統合性、正確度、信頼性を保証することを可能にします。再現性の実証能力、および解析結果元の追跡能力により、お客様は CLIA および / または CAP が求める基準をクリアすることができます。

- シーケンス装置から直接アップロードされた全データにチェックサムを実行し、ソースデータとの統合性を保証
- S3 のゲノムデータを含む全データが不変
- BaseSpace Sequence Hub アプリのバージョンをコントロール、公開されたアプリの改変を防ぐための手順を策定
- 検査結果の解釈を変更できる機能をバージョン化、ユーザーは新バージョンの検証が完了するまで前バージョンの使用を続けることが可能
- 詳細なログで、実行された解析をすべて描写

詳細について

BaseSpace Sequence Hub についての詳細、BeseSpace 無料アカウントへのサインアップは、jp.illumina.com/basespace をご覧ください。

参考文献

1. Amazon Web Services. aws.amazon.com.Accessed June 7, 2016.
2. BaseSpace Sequence Hub User Terms of Use. basespace.illumina.com/agreements/toc. Accessed June 7, 2016.
3. HHS Health Information Privacy. www.hhs.gov/hipaa/. Accessed June 7, 2016.
4. Centers for Medicate and Medicaid Services. www.cms.gov. Accessed June 7, 2016.
5. Clinical Laboratory Improvement Amendments (CLIA). www.cms.gov/Regulations-and-Guidance/Legislation/CLIA/index.html. Accessed June 7, 2016.
6. CAP Guidelines. www.cap.org/web/home/resources/cap-guidelines?_afrLoop=1191523387428127#!%40%40%3F_afrLoop%3D1191523387428127%26_adf.ctrl-state%3Dmcegq9mom_4. Accessed June 7, 2016.

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

代理店

Pub. No. 970-2016-J020 16SEP2016

illumina®