BaseSpace® Variant InterpreterおよびHIPAA

拡大可能なソリューションによってゲノムデータから迅速に生物学的情報を抽出

はじめに

BaseSpace Variant Interpreterは、簡単に使えるプラットフォームであり、ラボが効率的かつ正確に次世代シーケンス（NGS）データから生物学的な関連情報を抽出することができます。機密である保健関連情報を解析するすべてのプラットフォームは、データの安全性に対処する性能を備えていなければいけません。本テクニカルノートでは、BaseSpace Variant InterpreterによるHealth Insurance Portability and Accountability Act（HIPAA）（医療保険の携行性と責任に関する法律）の中枢のセキュリティ要件への対処方法について概説します。

HIPAAの背景

HIPAAは1996年に米国で成立されました。立法化された後、United States Department of Health and Human Services（HHS）（米国保健社会福祉省）は複数の規制を実行し、実際に法律が運用されています。HHSはHIPAAの順守を監視する規制機関でもあります。とりわけ、HIPAAでは保護対象保健情報（PHI）のセキュリティとプライバシーに対する国家規格が制定されました。HIPAAは、Health Information Technology for Economic and Clinical Health Act（HITECH Act）（経済的および臨床的健全性のための医療情報技術に関する法律）が立法化された2009年に大幅に更新されました。 HIPAAの重要な規則には、セキュリティ規則、プライバシー規則、情報漏えい時の通知規則があります。 HIPAA、HIPAAの歴史、具体的なHIPAA規制へのリンクに関する詳細については、HHSの保健情報プライバシーウェブサイト[1]をご覧ください。

BaseSpace Variant InterpreterおよびHIPAA

BaseSpace Variant InterpreterはHIPAAのセキュリティ規則要件を満たすよう設計され、運用されています。HIPAAのセキュリティ規則の要件は、電子保護保健情報（ePHI）の機密性、整合性、および安全性を確保するための管理上、物理的、および技術的な安全措置があげられます。BaseSpace Variant InterpreterはHIPAAのセキュリティ規則の中心的要素を満たすための性能を備えた設計となっており、イルミナはその要素を満たすための防御対策を行っています（表1）。

管理上の安全措置

BaseSpace Variant Interpreterは確立されたポリシー、手順、そして該当する場合、プラットフォーム内のデータの安全性を確保するために設計された技術的防御対策に従います。これらのポリシーは、最小限の従業員にデータへのアクセスを制限し、アクセス許可、確立、修正、およびアクセス終了のプロセスを処理する手順をサポートしています。バックアップ、ビジネスコミュニティ、および損害対応手順も文書化し、テストしています。

表 1: セキュリティ規則の防御対策

セキュリティ防御対策	内容
管理上の防御対策	リスク評価の実行
	リスクマネジメントポリシーの導入
	機密厳守を従業員に教育
	セキュリティ事故の報告
物理的防御対策	施設へのアクセス防御対策実施の必要性
	ワークステーション使用に関するポリシー
	モバイルデバイスへのポリシーおよび手順
	ハードウェアインベントリー
技術的防御対策	アクセスコントロール：固有のユーザー識別
	アクセスコントロール：緊急アクセス手順
	認証：ユーザー識別を検証するための認証手順
	転送セキュリティ：防御対策の整合性
	転送セキュリティ：暗号化

物理的安全措置

イルミナは、ISO 27001標準に基づいて承認され、HIPAAの防御対策要件を満たす、安全なアマゾンウェブサービス設備における情報技術インフラストラクチャー上にあるBaseSpace Variant Interpreterプラットフォームのホストです。この設備は、冗長性機能が内蔵されており、物理的なアクセス防御対策を順守しています。

技術的安全措置

BaseSpace Variant Interpreterは、アクセス防御対策から始まり、データの機密性と整合性を確保するために設計されたさまざまな技術的防御対策を実施しています。ネットワークトラフィックは、厳密に処理状態を把握したネットワークファイアウォールを経由して制限されています。本プラットフォームへの管理上のアクセスは制限されており、複数の認証を必要とします。プラットフォームへの全アクセスはログに記録され、モニターされます。データは、Transport Layer Security（TLS）（トランスポート層セキュリティ）プロトコールを使って、転送時（データがデータセンターから離れる際は常時）にはさらに保護されます。残りのゲノムデータおよびePHIはAdvanced Encryption Standard（AES）を使って保護されます。BaseSpace Interpeterは、脆弱性スキャンおよび不正侵入テストも行っています。

BaseSpace Variant Interpreterは、お客様がシステムとデータへのアクセスを制御しモニターできるセキュリティ性能も搭載しています。本ソリューションへのアクセスは、直接承認によるか、お客様のインフラストラクチャーによるシングルサインオンを経由して管理することができます。BaseSpace Variant Interpreterは、設定した期間で指定したアクセス失敗数の後、アカウントをロックアウトするよう設定することができます。パスワードの複雑性は、お客様のパスワードポリシーに合わせて設定することもできます。お客様は、ePHIおよびゲノムデータの作成、読み取り、更新および削除を含めたアカウントによるシステムへのアクセスを監査することができます。

詳細について

BaseSpace Variant Interpreterは、無料トライアルを期間限定で利用できます。詳細についてはwww.illumina.com/variantinterpreterにアクセスしてください。

参考資料

1. Health Information Privacyウェブサイト。 www.hhs.gov/hipaa. Accessed September 7, 2017.

イルミナ株式会社 •0800-111-5011 テクニカルサポート部（受付時間：平日9:00 - 17:00） • techsupport@illumina.com • jp.illumina.com

本製品の使用目的は研究に限定されます。診断での使用はできません。

Pub.No.970-2016-003-B JPN