

IEC 80001 概要

日本語

概要

使用目的

以下に示す情報は、施設の医療 IT ネットワークのリスク管理担当者向けのもので、IEC 80001-1:2010 および IEC 60601-1:2005+AMD1:2012 に従って業務を遂行できるようにするため。

この情報は以下のブレインラボ製品に適用されます。

	製品
プラットフォーム	<ul style="list-style-type: none">• Buzz• Curve ナビゲーションシステム(シーリングマウント)• Curve ナビゲーションシステム• Digital Lightbox• Kick ナビゲーションシステム(磁場式)(Kick EM)• Kick ナビゲーションシステム(光学式)• iPlan Net (3.6, 3.7)• Origin Server (3.x)• コールブリナビゲーションシステム 2.x• ベクタービジョンコンパクト• ベクタービジョンスカイ• ベクタービジョンスクエア
RT 患者ポジショニング	<ul style="list-style-type: none">• ExacTrac
ソフトウェア	<ul style="list-style-type: none">• Brainlab Elements 全製品• Brainlab ナビゲーションソフトウェア全製品• タッチスクリーン PC 用 DICOM Viewer• iPlan 3.0 (Cranial/ENT/CMF/Stereotaxy/Flow/Spine/View)• iPlan RT (4.1, 4.5)• Qentry

IT ネットワークに組み込まれることを意図した PEMS(プログラマブル電気医用システム)

他の機器が含まれている IT ネットワークにブレインラボ製品を接続すると、患者、操作者、または第三者に対し、これまで未確認のリスクが生じる可能性があります。

このようなリスクについては、責任組織が特定、分析、評価を行い、コントロールする必要があります。その後の IT ネットワークの変更は、新たなリスクを招く恐れがあり、さらなる分析が必要になります。IT ネットワークの変更に含まれるものは以下のとおりです。

- IT ネットワーク構成の変更
- IT ネットワークへの追加アイテムの接続
- IT ネットワークからのアイテム切り離し
- IT ネットワーク接続機器の更新/アップグレード

適用可能なグループポリシー設定

システムが正しく機能するためには、システムを(ドメインコントローラーなどで)院内ネットワークに導入する際には以下の Windows 10 のグループポリシー設定を変更しないでください。

該当する設定のパスは以下の通りです。

Computer/Policies/Administrative Templates:

- Control Panel/Personalization
- Control Panel/User Accounts
- System/Device Installation
- System/Logon
- System/Internet Communication Management
- System/Power Management
- System/Shutdown
- Windows Components/AutoPlay Policies
- Windows Components/Desktop Window Manager
- Windows Components/Event Log Service
- Windows Components/Internet Explorer/Security Features/Add-on Management
- Windows Components/Windows Defender/Exclusions
- Windows Components/Windows Update

ネットワーク接続の技術仕様

ブレインラボ製プラットフォームには、以下の IT ネットワーク接続を特徴として備えています。

	全プラットフォーム	一部プラットフォーム
リンク層	≥ 1 イーサネットポート、100/1000BASE-T ネットワークに対応	• イーサネットポート、1000BASE-T ネットワークに対応 • IEEE 802.11b/g/n/ac に対応する WLAN
インターネット層	Ipv4 接続	Ipv6 接続

注記:互換性の詳細については該当するユーザーガイドを参照してください。

製品の設定

ブレインラボのサービスエンジニアが設置、設定した製品は(技術的、合理的に適用可能な限り)、IT セキュリティーの観点からは Microsoft Baseline Security Analyser (MBSA) に準拠しています。

初期設定後の変更は製品の安全性および有効性に影響を及ぼす可能性があるためご注意ください。

必要な IT ネットワーク構成

本書に一覧表示している IT ネットワークの仕様に基づき、ファイアウォールを設定する必要があります。

ブレインラボでは、不正アクセスから保護されていないネットワークは fault-prone とみなされます。

IT ネットワーク障害が引き起こすリスク

非タイムクリティカルなサージカルプランニングを実施する際には障害は危険な状況を引き起こしません。

ただし、IT ネットワーク接続に障害が生じると治療は中断され、やり直しが必要となる可能性があります。障害発生時に

ExacTrac を使用すると、患者に不要な KV イメージングを実施することになりかねません。

また、ブレインラボ製品への術中 DICOM push(モダリティーまたは C-arm から)が失敗すると、患者の治療にブレインラボ製品を使用できなくなります。

技術的解説とユーザーガイド

お使いの製品プラットフォームに応じて以下の資料をご利用いただけます。

- DICOM Conformance statements (DICOM 適合性宣言書)
- FDA and CE declarations (FDA および CE の宣言書)
- IT Network Planning (IT ネットワークプランニング)
- Navigation Software User guide (ナビゲーションソフトウェアユーザーガイド)
- System & Technical User Guide (システム & テクニカルユーザーガイド)
- Clinical User Guide (クリニカルユーザーガイド)
- Technical specification sheet (技術仕様シート)

お問い合わせ先

製品の回収について

ブレインラボは異常が確認された場合、すべてのお客様にお知らせします。

サイバーセキュリティに関する通告

ブレインラボはサイバーセキュリティの問題が確認された場合、すべてのお客様にお知らせし、適宜ソフトウェアアップデートを提供します。



IEC 80001 概要

意図される情報フローと IT ネットワークの仕様

対象製品	IT ネットワークに接続する目的	IT ネットワークの要件		セキュリティ仕様				
		可用帯域幅	追加帯域幅	規格	ポート			
全製品	医療イメージングデータのロード	≥ 100 M ビット/秒 (推奨: ≥ 1 G ビット/秒)	ディスク容量: ≥ 250 GB (推奨: SSD)	DICOM	• 104/TCP (外部接続から遮断) • 11112/TCP		受信 & 送信	
	医療イメージングデータの保存			CIFS	445/TCP			
	HTML5 アプリケーションへのリモートアクセス	≥ 10 M ビット/秒	レイテンシー < 100 ms	• HTTP • HTTPS	• 44388/TCP/UDP • 55581/TCP/UDP		受信	
	リモートサポート	≥ 2 M ビット/秒	• インターネットアクセス • レイテンシー < 100 ms	iHelp® (Axeda)	443/TCP	認証サーバー	support.brainlab.com	送信
						ヨーロッパ	gas-de2.axeda.com gas-de3.axeda.com gas.ie1.axeda.com gas.ie2.axeda.com	
南北アメリカ						ghsom1.axeda.com gas-bo3.axeda.com gas-bo7.axeda.com ghsj1.axeda.com ghsj2.axeda.com		
アジア太平洋地域						ghjap1.axeda.com ghjap2.axeda.com gas-aus2.axeda.com gas-aus3.axeda.com gas-cne4.axeda.com gas-cne6.axeda.com		
英国						ghuk2.axeda.com ghuk3.axeda.com		
Qumenty クラウドへのアクセス	≥ 2 M ビット/秒 (推奨: 10 M ビット/秒)	N/A	Qumenty		servicesus1.qumenty.com v01-us1.qumenty.com v02-us1.qumenty.com			
Buzz リモートコントロール	≥ 15 M ビット/秒	WLAN 接続	Brainlab リモートコントロール	55578/TCP		受信		
データリンクの確立	N/A	N/A	mDNS / DNS-SD	5353/UDP (マルチキャスト 224.0.0.251)				
プラットフォーム	イメージングモダリティの接続	≥ 1 M ビット/秒	最低限のレイテンシーのための同じブロードキャストドメイン内での接続	Brainlab C-arm	7915/TCP	受信 & 送信		
	ナビゲーション情報の転送			NTP	• 44445/TCP/UDP • 55555/TCP/UDP • 56666/TCP/UDP			
				OpenIGTLink	123/UDP	送信		
	セッション共有	≥ 1 G ビット/秒			• Brainlab flex Backbone	22222/TCP	受信	
	ビデオストリーム、録画、会議機能	≥ 40 M ビット/秒		N/A	• HTTP • HTTPS • SDP • RTP • RDP • HTTPS	• 57575/TCP • 57574/TCP • 50001/TCP • 57581/TCP • 50002/UDP • 57578/TCP/UDP		
					• LDAP • LDAP SSL • LDAP GC • LDAP GC SSL • Kerberos • DNS • Microsoft-DS Kerberos パスワードの変更	• 3389 (構成可能)/TCP • 443/TCP • 8080/TCP		
リモートデスクトップ接続 (Origin Server でのみ使用可能)	≥ 1.5 M ビット/秒	レイテンシー < 100 ms				送信		
• プラットフォーム • RT 患者ポジショニング	ユーザー認証	N/A	Microsoft Active Directory®	• Microsoft-DS • Kerberos • LDAP • DNS	• 389/TCP/UDP • 636/TCP/UDP • 3268/TCP • 3269/TCP • 88/TCP • 53/TCP/UDP • 445/TCP/UDP • 464/TCP	送信		
	Windows®ドメインインテグレーション			• VNC	• 445/TCP/UDP • 389/UDP • 53/TCP/UDP • 88/TCP/UDP			
RT 患者ポジショニング	サードパーティー製コンピュータとの接続	≥ 1 M ビット/秒	N/A	Varian ADI	5900/TCP	受信		
	linac との接続	N/A	• レイテンシー < 100 ms • 完全なスイッチネットワーク	Elekta	56050/TCP	受信 & 送信		
				Varian	• 135/TCP • 1801/TCP • 2101/TCP			
ファイアウォールの構成		サードパーティー社製機器	Elekta (例: NSS)	56050/TCP 9090/TCP				