仮想環境に対応 Virtual VIP

Citrix/VMware/Parallels





指静脈認証に対応した LinuxOS端末から Windows10を利用することもできます。





指静脈認証のVIPを利用するシンクライアント端末のOSはLinuxです。MicrosoftのOffice製品、ExcelやWordを利用できないはずですが、Virtual VIPを利用することで、安全に仮想環境にログインができます。



動作環境

認証サーバ

OS	下記のいずれか(64ビットのみ対応) Windows Server® 2012 R2 Standard Update Windows Server® 2012 Standard Windows Server® 2008 R2 Standard SP1 Windows Server® 2008 R2 Enterprise SP1
前提プロ グラム	(64ビットのみ対応) Java SE Runtime Environment 8(JRE8)
データ ベース	以下のソフトウェアが既に導入されている場合は、 VIPインストールパッケージに含まれておりますため 導入前に削除してください。 PostgreSQL 9 Apache Tomcat 8

クライアント

OS	64ビット	Windows® Vista / Windows® 7 / Windows® 8 / Windows® 10 COS(Centerm Linux)	
前提プログラム		無し	
認証装置		mofiria FVA-U3SX	

保守サポート

保守サポートサービス営業時間

電子メール受付時間: 随時 対応時間: 9:30-12:00 および 13:00-17:00 休業日: 土曜日・日曜日、国民の祝日および弊社規定の休業日

74,

T4U株式会社 〒103-0025 東京都中央区日本橋茅場町1-8-3郵船茅場町ビル TEL 03-6661-7741 FAX 03-6661-7743 Mail info@t4u.asia Web www.t4u.asia

VIP

指静脈認証システム

Vein Identification Platform



- ♦ 静脈認証で確実な本人の特定。
- **◆ シンクライアント端末で情報漏洩の防止。**
- ◆ 細かなアクセス制御オプション。
- ◆ 自動暗号化ソフトと連携。
- ◆ 完全なログの記録。



シンクライアント端末で、外的要因の脅威は 防ぐことができる。 でも、そのシンクライアントは

「誰が操作しているのか。」

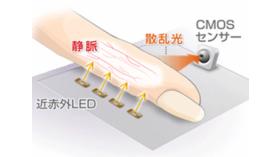
IoT時代は「本人の特定」が確実でなければならない。

本人の特定は「識別」と「認証」の2ステップ。

現在の本人の特定としては、IDで本人を識別し、パスワードでそれが本人であるのかを認証するしくみですが、様々なモノに本人の特定が必要となるIoTの時代において、IDとパスワードの運用は不可能です。

最先端の生体認証は指静脈!

認証は安価におさえることよりも、確実であることを重視する傾向が増しています。また、指紋認証の限界と新技術である指静脈の存在が高まり、指紋から静脈への置き換えを含み、指静脈認証の存在感が増してます。 静脈認証の確実性は高く、静脈内を流れる血液中の還元へモグロビンが吸収する近赤外線をあてて指を撮像し、静脈パターンを抽出します。この静脈パターンを予め登録された静脈パターンとマッチングすることで、認証を行ないます。 静脈認証方式は生体認証の中でも高い認証精度があります。



◆指の内部情報である!

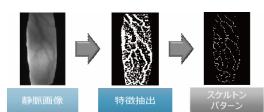
ドライ、ウェット、荒れ、傷等に影響されることが少い。

◆偽造・なりすましが極めて難しい!

表面情報である指紋のようにテープや粘土のようなものに残すことも出来ず、顔認証のように 外部情報でないため、偽造やなりすましが極めて困難。

	認証精度	偽造しにくさ	経年変化	機器のサイズ	価格
静脈	©	0	0	0	0
指紋	0	Δ	Δ	0	0
顔	Δ	Δ	Δ	Δ	Δ
虹彩	0	0	0	Δ	Δ
音声	Δ	Δ	Δ	0	0

VIP の指静脈認証技術



T4Uの指静脈認証システム VIPは、 認証精度が高い反射散乱方式採用の 静脈認証デバイスを採用。

※ パターンとして保管される指静脈情報は、暗号化もされているため、 個人情報として特定されることはありません。

静脈内の「還元ヘモグロビン」が吸収する近赤外線を当て撮影

効果的なエンドポイントプロテクション

T4U株式会社 End Point Protection System

シンクライアント + 生体認証 による効果。

◆ エンドポイントプロテクション

シンクライアントシステムや仮想環境の普及に伴い、アクセスする端末管理には一定の制御・管理対応がされていますが、ユーザーのなりすまし対策は不十分です。 シンクライアントと指静脈認証システムをあわせて導入することで、エンドポイントのセキュリティレベルを、ある一定レベルから確実なものへと向上させることが可能となります。



- ◆パソコン、シンクライアントから、 指静脈認証のみで社内システムに ログインできる。
- ◆パスワードの管理が不要で、サーバー 側から端末・ソフトも一括管理可能。
- ◆指静脈システムの全口グが自動的に 取得される。

◆ 情報システム部門とユーザーの負担が大幅減。

パスワード運用に伴う、ユーザーへのパスワード紛失への対応や再発行、管理対応が無くなります。シンクライアントを導入することでユーザー側の端末メンテナンス作業が減ります。また、シンクライアント管理機能を利用すると、サーバー側から一括でアプリケーション、端末を管理することが可能です。端末側で発生したトラブルへのサポート対応もリモート操作で対応できます。



	情報システム部門	ユーザー	
運用面	・パスワードの再発行、紛失等のユーザーからの問合せなど ログイン時のサポート作業が激減。 ・サーバー側から一括管理ができる。	 ・面倒なパスワードが不要。 ・ログイン時間と手間の短縮。 ・端末導入ソフトの更新等のメンテナンスが不要。 ・ハイパフォーマンスなシンクライアント端末で、 ストレスフリーに。 ・リモート接続で、在宅勤務にも最適。 	
安全面	・ユーザー側での人為的、物理的な情報漏洩リスク減。 ・システム管理者のなりすましも発生しない。 ・事故時のログ情報も自動取得可能。	・ログインに必要な情報(パスワードやICカード等)を盗まれる可能性が ゼロになる。 ・端末に情報が残らないため、端末を盗まれても情報漏洩は発生しない。	

VIP のオプション

◆Web アプリケーションの提供。

VIPは、Webアプリケーションへのログインに指静脈認証をご利用いただけます。お客様独自のアプリケーションにもカスタマイズ対応します。

◆入退出システムとの連携。

社内システムへのログインだけでなく、オフィスへの入退出も指静脈認証を利用できます。オフィスに出社したユーザーだけが社内システムにログインできるよう制限をかけたり、社内システムにログインしているユーザーだけが特定のドアに入室できるような仕組みも準備できます。