



VP-II XTM

Hand Vascular Pattern Recognition

操作リファレンス



1. 手の入力方法
2. 認証・登録・再登録・削除方法
3. 状態通知機能説明書
4. VP-II X取扱説明書
5. NetControl-X取扱説明書
6. VP-II XG取扱説明書

株式会社SYNCHRO



登録および認証時の正しい手の入力方法

登録および認証の処理を正しく実行するためには、常に一定の位置で手を認証装置に入力する必要があります。

使用者は初回登録時に確認のため認証を数回繰り返してください。認証が正しく行なわれた場合は、以降も認証装置を正常に使用することができます。この時点で認証がたびたび失敗する場合、登録時の手の位置が正しくない可能性があります。この場合は、別紙に記載した手順に従って手を正しい位置で入力し、再登録を行ってください。

使用者は認証装置に手を入れる際に一定の距離と正しい姿勢を維持しなければなりません。位置がずれると手の甲の静脈パターンに歪みが生じ、読取ったイメージも変わってしまいます。その結果、使用者の認証に失敗する可能性があります。

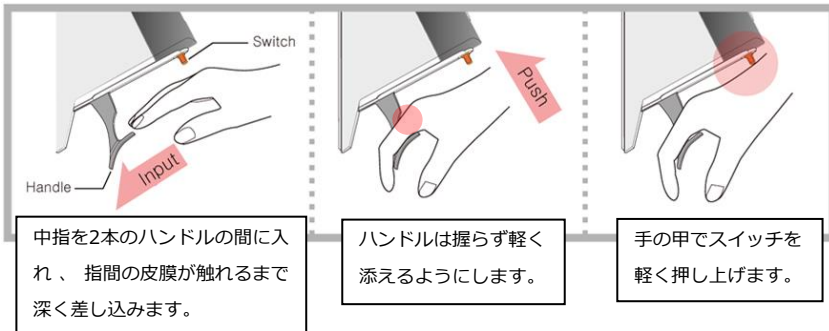
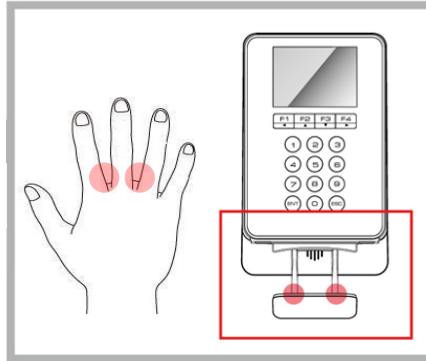
ハンドルは、センサ部で静脈パターンのイメージを読み取る際に、使用者の手を正しい位置に固定します。

ハンドルは水平のバーで、認証装置本体と2本の柱を介して結合しており、認証時には2本の柱の間に手の中指を付け根まで入れて軽く乗せ、手の位置を固定させます。次いで、センサカバーの前部に埋め込まれているスイッチがトリガスイッチです。トリガスイッチの位置は、使用者の手が適切な位置に入ったとき手の甲で容易に押せるよう設計されています。手の甲を軽く持ち上げ、認証装置のセンサカバーの前部に埋め込まれているトリガスイッチを押し、認証操作を開始します。

尚、ハンドルは絶対に強く握らないでください。

手の入力方法

中指を2本のハンドルの間に入れます。指間の皮膚が触れるまで深く差し込んでください。その時にハンドルを握らず力を抜いてハンドルの上に軽く乗せてください。

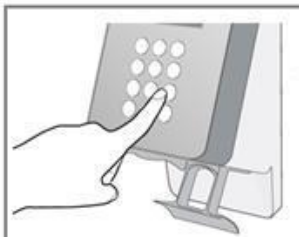


- 手首をトリガスイッチのほうにゆっくり持ち上げて、スイッチを押します。ハンドルを握らないでください。

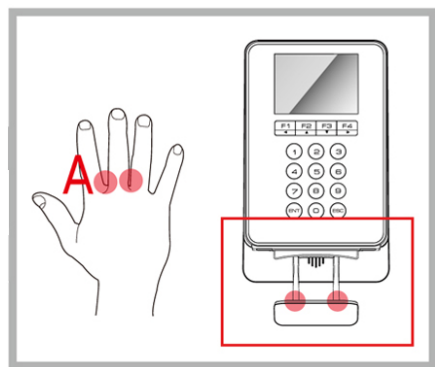
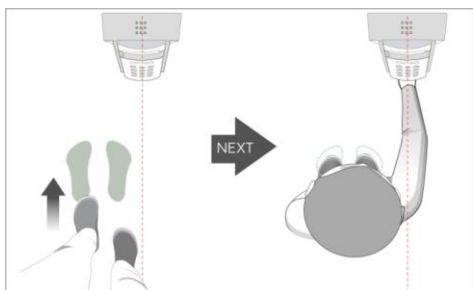
注意事項



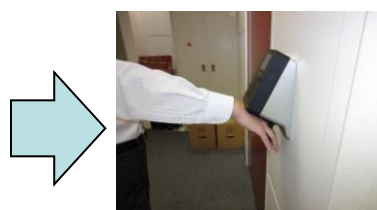
VP-II 認証方法



【PINの入力】



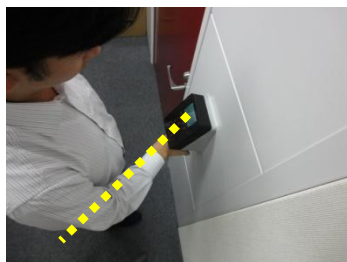
バーの根元まで
手を入れます



手の甲をゴムの
カバーに押し当てます

■ 注意事項

手はまっすぐ入れてください
横から手が入ると認証エラーが発生しやすいです。



手が斜めに入っている



肩から



手の差込みが浅い



手の股がバーに当たる
まで差し込んでください



認証に成功しました



認証に失敗しました
手の位置を確認して
もう一度認証してください

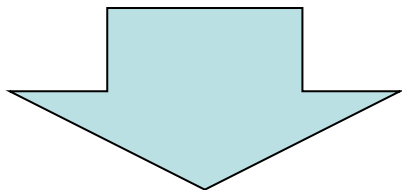
VP-II X登録方法

【管理者の認証】

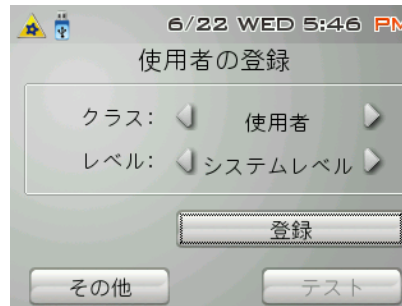
PIN + F1キーで管理者認証します



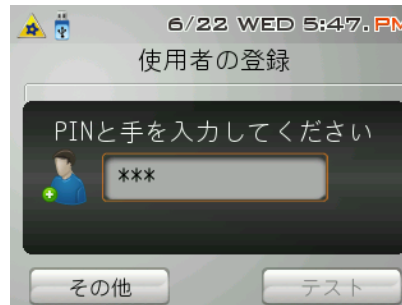
- ①PIN入力後F1 (Manager)を押します ②手をスキャンして認証します



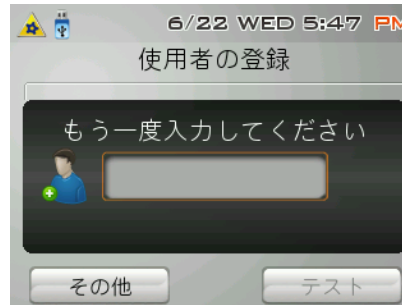
管理メニューが表示されますので
「使用者管理」 - 「使用者の登録」を選択してください



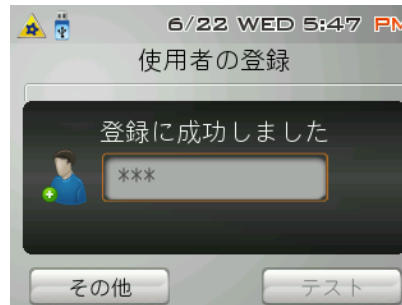
使用者の登録画面が
表示されますので、
登録ボタンを押してください



登録する使用者のPINを入力して
手の甲をスキャンしてください



登録する方のPINを入力して
手の甲をスキャンしてください



登録に成功しました

VP-II X再登録方法

【管理者の認証】

PIN + F1キーで管理者認証します



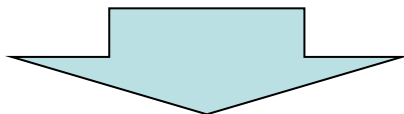
<注意>
PIN入力前にF1を押下すると勤怠管理の出勤操作になります。

①PIN入力後F1 (Manager)を押します

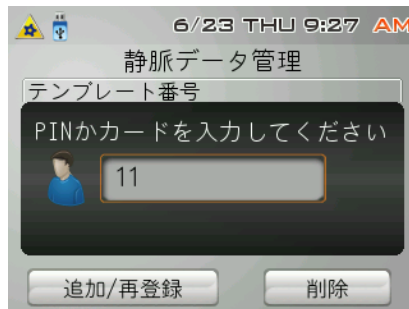
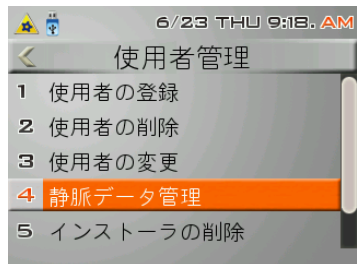
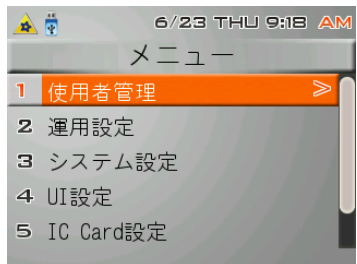


<注意>
管理者に割り当てられていないユーザが認証すると「未登録ID」のエラーを表示します。

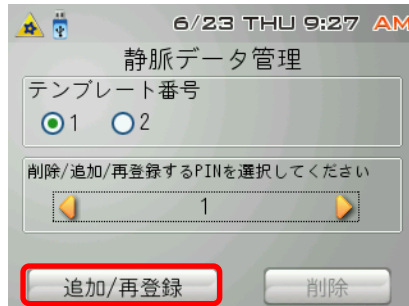
②手をスキャンして認証します



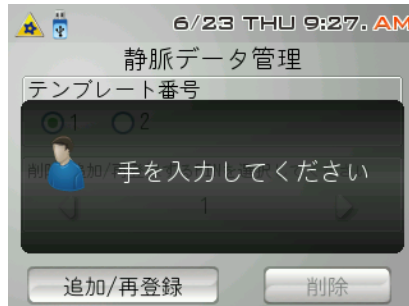
管理メニューが表示されますので「使用者管理」-「静脈データ管理」を選択してください



再登録する使用者のPINを入力してENTを押してください

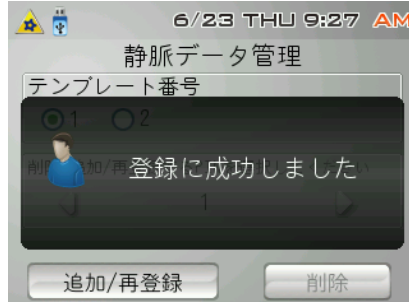


追加/再登録を選択して押してください



確認メッセージが表示されるのでよろしければENTボタンを押してください

手を入力してください(×2回)



再登録に成功すると左図のメッセージが表示されます

VP-II X削除方法

【管理者の認証】

PIN + F1キーで管理者認証します



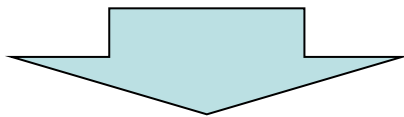
<注意>
PIN入力前にF1を押下すると勤怠管理の出勤操作になります。

①PIN入力後F1 (Manager)を押します

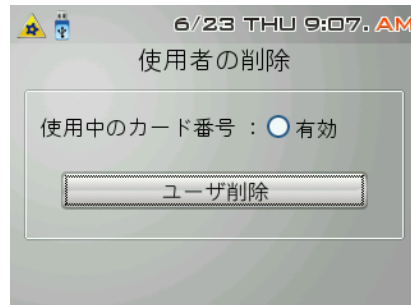
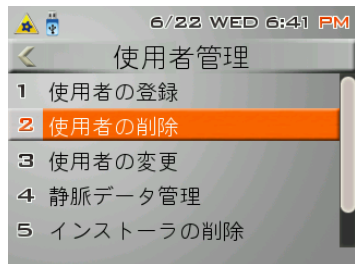
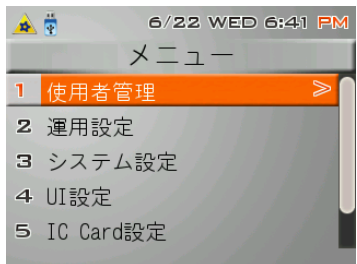


<注意>
管理者に割り当てられていないユーザが認証すると「未登録ID」のエラーを表示します。

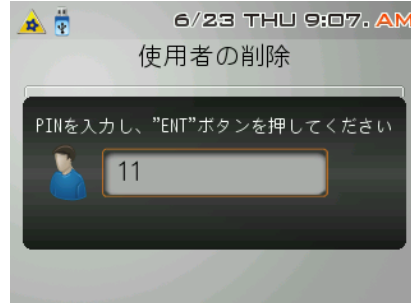
②手をスキャンして認証します



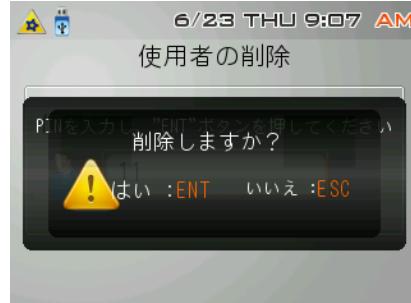
管理メニューが表示されますので「使用者管理」－「使用者の削除」を選択してください



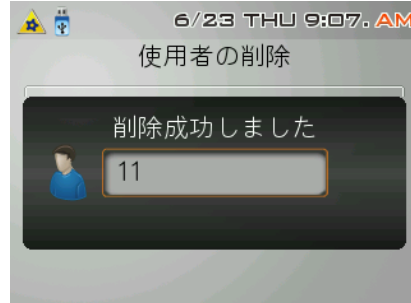
使用者の削除画面が表示されますので、削除ボタンを押してください



削除する使用者のPINを入力して「ENT」ボタンを押してください

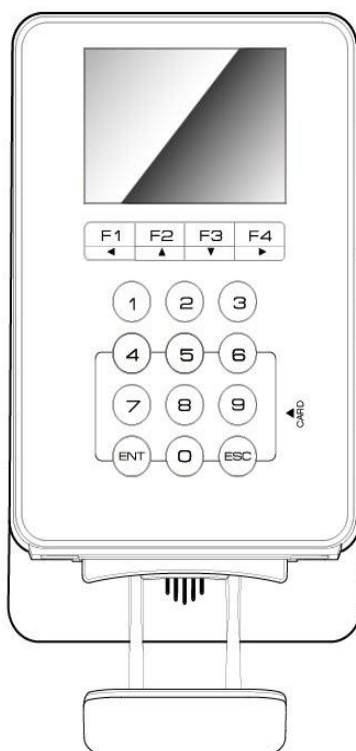


確認メッセージが表示されるのでよろしければENTボタンを押してください



削除に成功すると左図のメッセージが表示されます

手の甲静脈認証システムVP-II X VP-IIX、XG、NetControl-X Hand Vascular Pattern Recognition System



状態通知機能説明書 Ver.1.1



Hand Vascular Pattern Recognition

はじめに

手の甲静脈認証システム VP-II X をお買い上げいただき、まことにありがとうございます。

このガイドは、VP-II X システムの操作説明書別冊「状態通知機能説明書」です。

□ カスタマーサービス

設置済み製品の構成を追加または拡張する場合、または修理や保守が必要である場合は、設置担当者、または製品の販売店にご連絡の上、熟練した技術者の支援を得てください。テクニカルサポートやその他のサービスの詳細については、販売店にお問い合わせください。

株式会社 SYNCHRO

〒102-0073 東京都千代田区九段北 1-10-9 九段 VIGAS 5 階

Tel: 03-4570-3291 FAX: 03-4570-3292

電子メール: message@udc-synchro.co.jp

Web: www.udc-synchro.co.jp

□ 免責事項

本書に記載されている内容は情報提供のみを目的としています。Techsphere は、不正確または不完全な情報に対して、およびこれらの情報を信頼して行われた行為に対して、一切の責任を負いかねます。

注意: この説明書の内容は、製品の性能向上を反映するために、変更されることがあります。

□ 著作権について

本書は独占所有物です。参照以外の目的では使用しないでください。Techsphere Co., Ltd. はいかなる時点でも、この製品を変更または製造を停止する権利を保有しています。

改訂情報

□ V1.0: 2013 年 11 月

- 初版発行
- 1.1 版発行 VP-IIx マスタ/スレーブ運用について追記

目 次

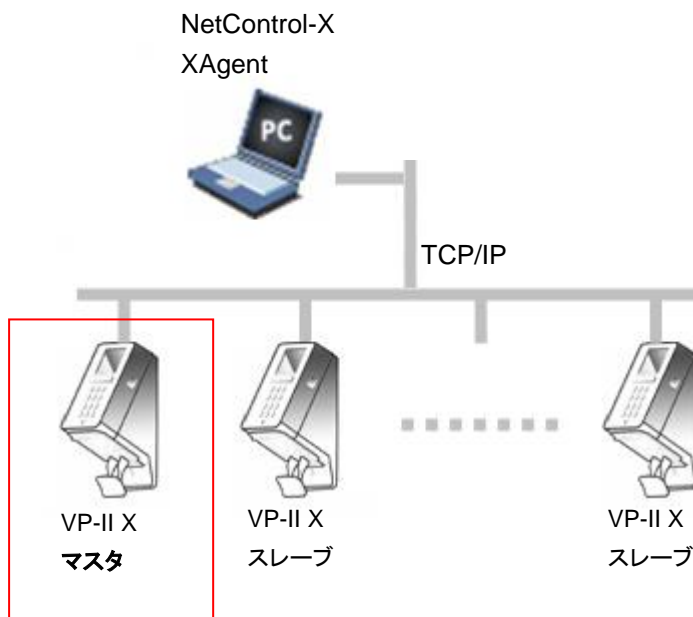
はじめに	2
改訂情報	3
目 次.....	4
1. VP-II Xのマスター/スレーブ運用について	5
2. VP-II Xの状態通知機能	6
3. XGの状態通知機能	7
4. NetControl-Xの状態通知機能.....	8

1. VP-II X のマスタ/スレーブ運用について

複数の VP-II X がネットワークに接続されている場合、そのうちの 1 台をマスタとして設定し、残りをスレーブとして設定する必要があります。XAgent が実行されているサーバをマスタとして設定することもできます。その場合、VP-II X ユニットはすべてスレーブに設定されます。

マスタは、ネットワーク全体に対する使用者のデータベース(静脈データ)を管理します。1つのネットワークにつき、マスタは1つのみである必要があります。

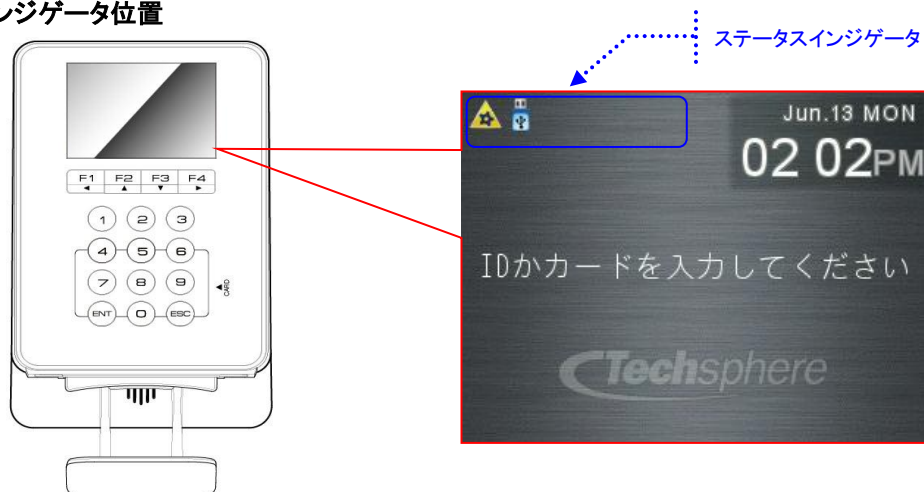
・VP-II X ネットワーク構成図



2. VP-II X の状態通知機能

VP-II X のステータスはスキャナのステータスインジゲータにアイコンで表されます。

・ステータスインジゲータ位置



・アイコン説明

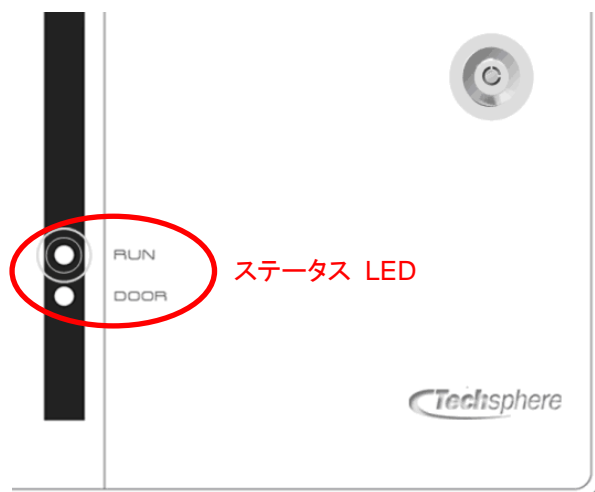
アイコン	ステータス	ヒントとトラブルシューティング
	ネットワークに接続されていません	<ol style="list-style-type: none"> 1. ネットワークケーブルの接続を確認してください。 2. 現在のシステムでのネットワーク設定を確認してください。 ⇒ IP アドレス、ゲートウェイ、サブネットなど。 3. ping コマンドを使って、ネットワークステータスを確認してください。 4. ネットワーク管理者に問い合わせてください。
	サーバに接続されていません	<ol style="list-style-type: none"> 1. サーバの設定を確認してください。 2. サーバのステータスを確認してください。 3. ネットワーク管理者に問い合わせてください。
	マスタに接続されていません	<ol style="list-style-type: none"> 1. 管理者メニューでマスタの設定を確認してください。 2. マスタのステータスを確認してください。 3. ネットワーク管理者に問い合わせてください。
	タンパースイッチからの警告です	<ol style="list-style-type: none"> 1. VP-II X のステータスを確認してください。 2. VP-II X の設置状態およびタンパースイッチ設定を確認してください。 3. タンパースイッチが機能していることを確認してください。
	テストモード	<ol style="list-style-type: none"> 1. VP-II X はテストモードで動作しています。テストモードを解除すると、このアイコンが表示されなくなります。
	VP-II XG が接続されていません	<ol style="list-style-type: none"> 1. VP-II XG と VP-II X の間の接続を確認してください。 2. VP-II XG のステータスを確認してください。 3. VP-II XG の設定を確認してください。
	USB メモリが接続されています	<ol style="list-style-type: none"> 1. USB メモリが接続されています。

3. XG の状態通知機能

VP-II XG のステータスはステータス LED により表示されます。

VP-II XG の状態を示す LED は以下で説明するように作動します。

・ステータス LED 位置



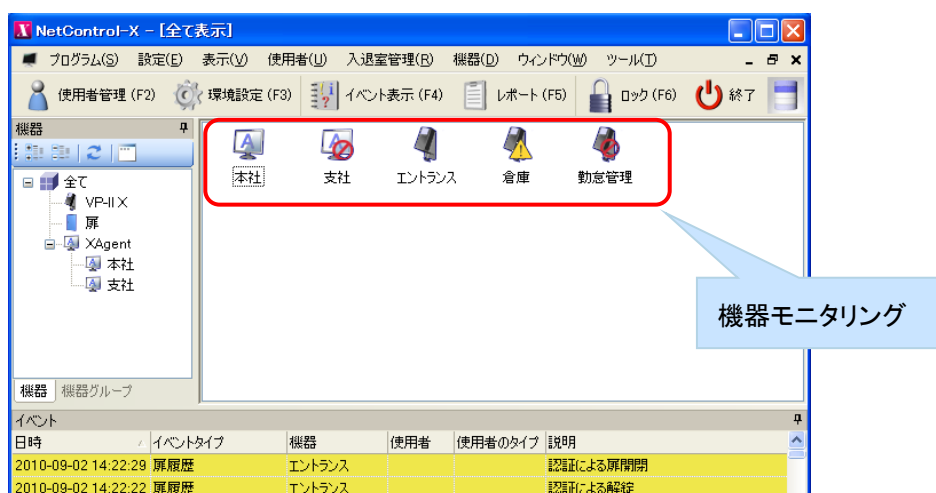
・ステータス LED 説明

LED	Status	
RUN	消灯	電源 OFF 時
	緑点滅(低速)	ペアリング未設定時(通信異常時、または初期出荷時)
	赤/緑/橙点滅(高速)	ペアリング設定時(通信正常時)
DOOR	消灯	解錠信号未入力時
	橙点灯	解錠信号入力による解錠時

4. NetControl-X の状態通知機能

NetControl-X ではメイン画面の機器モニタリングにて各機器の状態を把握することができます。

・機器モニタリング(メイン画面)



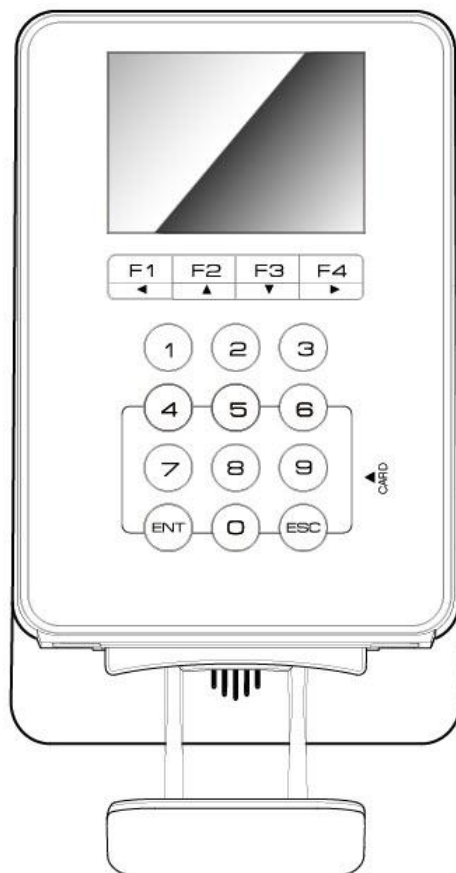
・アイコン説明

	DBMS 接続ステータス: 青(接続中)／赤(未接続)。
	XAgent ステータス(正常／エラー)。
	VP-II X は正常に動作しています。
	VP-II X は接続中ですが、正常に動作していません。たとえば、マスタに接続できていないか、XG が使用されているときに XG と接続されていないか等。アイコンの上にマウスポインタを重ねると、エラーの詳細が表示されます。
	VP-II X エラー(未接続)。
	扉が施錠(施錠)している時。 ※XG にステータス入力が必要となります。
	扉が開扉(解錠)している時。 ※XG にステータス入力が必要となります。
	扉施錠エラー ※XG にステータス入力が必要となります。
	アイコンの背景に表示される色付きの帯には次のような意味があります。 グリーン: 開放時間帯が設定されている(開放時間帯には扉は解錠されたままです) オレンジ: バイパス機能が使用されている(使用者は PIN またはカードのみで出入許可を得られます) グレー: 扉閉鎖コマンドにより扉が施錠されている(使用者が認証しても扉は解錠されません)

Hand Vascular Pattern Recognition System

VP-II X

Hand Vascular Pattern Recognition System



取扱説明書

Ver.1.5

Techsphere

SYNCHRO

HVPR

Hand Vascular Pattern Recognition

はじめに

手の甲静脈認証システム VP-II X をお買い上げいただき、まことにありがとうございます。

この説明書では、VP-II X の特徴や機能について説明いたします。最高のパフォーマンスを得るには、ご使用を開始する前に、この説明書全体をお読みいただくことをお勧めします。

VP-II X は生体認証スキャナで、赤外線ベースのセンサ機器を使用して、手の甲の表皮の下にある下皮から読み取った、個人個人で異なる静脈パターンを利用して、使用者を認証します。静脈パターンは裸眼では見えず、手の傷や汚れには簡単に影響されません。このため、条件の厳しい環境でもパフォーマンスが低下せず、改ざんは 100%不可能で、他の生体認証方式に伴うプライバシーの問題もありません。HVPR テクノロジーの利用により、全人口の 99.98%が認証速度 0.4 秒でシステムを正確に使用することができます。使用者によるボトルネックが解決され、別の通用口を用意する必要がなくなります。

VP-II X は、サーバや他の VP-II X 機器との通信に TCP/IP ネットワークを使用します。IP アドレスは、ローカルエリアネットワークに接続したときに、DHCP により自動的に取得されます。他入退室管理システム (PACS) への基本インターフェースは Wiegand で、RS485 と RS232 がオプションとしてサポートされています。

VP-II X は、スタンドアロンシステムとして、または TCP/IP ベースのネットワーク上で動作し、TCP/IP、Wiegand、RS232、RS485 を通じて外部システムへの各種インターフェースを提供します。また、サーバで稼動するアプリケーションソフトウェアも提供されます。

□ カスタマーサービス

設置済み製品の構成を追加または拡張する場合、または修理や保守が必要である場合は、設置担当者、または製品の販売店にご連絡の上、熟練した技術者の支援を得てください。テクニカルサポートやその他のサービスの詳細については、販売店にお問い合わせください。

株式会社 SYNCHRO

〒102-0073 東京都千代田区九段北 1-10-9 九段 VIGAS 5 階

Tel: 03-4570-3291 FAX: 03-4570-3292

電子メール: message@udc-synchro.co.jp

Web: www.udc-synchro.co.jp

□ 免責事項

本書に記載されている内容は情報提供のみを目的にしています。Techsphere は、不正確または不完全な情報に対して、およびこれらの情報を信頼して行われた行為に対して、一切の責任を負いかねます。

注意: この説明書の内容は、製品の性能向上を反映するために、変更されることがあります。

□ 著作権について

本書は独占所有物です。参照以外の目的では使用しないでください。Techsphere Co., Ltd.は、いかなる時点でも、この製品を変更また製造を停止する権利を保有しています。

目次

はじめに.....	1
目次.....	2
目次.....	2
改訂情報.....	5
第1章 概要.....	5
1. VP-II X スキャナ.....	5
2. ネットワーク構成.....	6
2.1 マスタ/スレーブ運用.....	6
2.2 ネットワーク設定.....	7
3. VP-II Xの仕様.....	8
4. 手の入力についてのガイドライン.....	10
第2章 登録、削除、認証.....	11
1. 管理者メニュー.....	11
1.1 管理者.....	11
1.2 インストーラ.....	11
1.3 テストモード.....	11
1.4 インストーラの登録.....	11
1.5 管理者メニューへのアクセス.....	12
1.6 管理者メニューの主な使い方.....	12
1.7 メニューツリー.....	12
2. 登録.....	14
2.1 使用者タイプ.....	14
2.2 使用者/管理者の登録.....	15
3. 削除.....	17
3.1 インストーラの削除.....	17
3.2 使用者の削除.....	17
4. 認証.....	18
4.1 管理者の認証.....	18
4.2 パスワード使用者の認証.....	19
4.3 ジョブコードの入力.....	19
4.4 カード番号を使った認証.....	19
4.5 機能キーを使った認証.....	19
4.6 脅迫警報コードを使った認証.....	19
4.7 インストーラの認証.....	20
5. 使用者情報の変更.....	20

5.1	使用者の変更	20
5.2	静脈データ管理(静脈データの追加/再登録)	22
第3章 環境設定		24
1.	ネットワーク設定	24
1.1	ネットワーク環境の設定(TCP/IPパラメータ)	24
1.2	マスタ/スレーブ設定	24
1.3	サーバ設定	26
1.4	スレーブリスト	27
2.	システム設定	28
2.1	日付/時刻設定	28
2.2	ファームウェア情報	28
2.3	VP設定(セキュリティレベル、生体検知、認証試行回数)	29
2.4	ドア設定	29
2.5	サマータイム	31
2.6	システム初期化(工場出荷設定にリセット)	31
2.7	施錠検知設定	32
2.8	AUX設定	32
2.9	1扉の入退認証モード	33
3.	運用設定	34
3.1	モード設定(ネットワーク/シリアル)	34
3.2	テストモードの解除	34
3.3	キーパッド入力設定	34
3.4	スリープモード	35
3.5	タンパースイッチ設定	35
3.6	DB検索オプション	36
3.7	勤怠管理設定	36
4.	UI設定	37
4.1	言語設定	37
4.2	サウンド設定	37
4.3	PIN表示オプション	38
4.4	時計表示	38
5.	IC Card設定	39
5.1	Wiegand設定	39
5.2	MIFARE/iClassカード	41
5.3	ASI4000設定	43
5.4	DUALI設定	43
5.5	PACS(Physical Access Control Security)設定	43
6.	ツール	45
6.1	DBバックアップ/リストア	45
6.2	診断ツール	46
6.3	ソフトリセット	47
第4章 付録		48

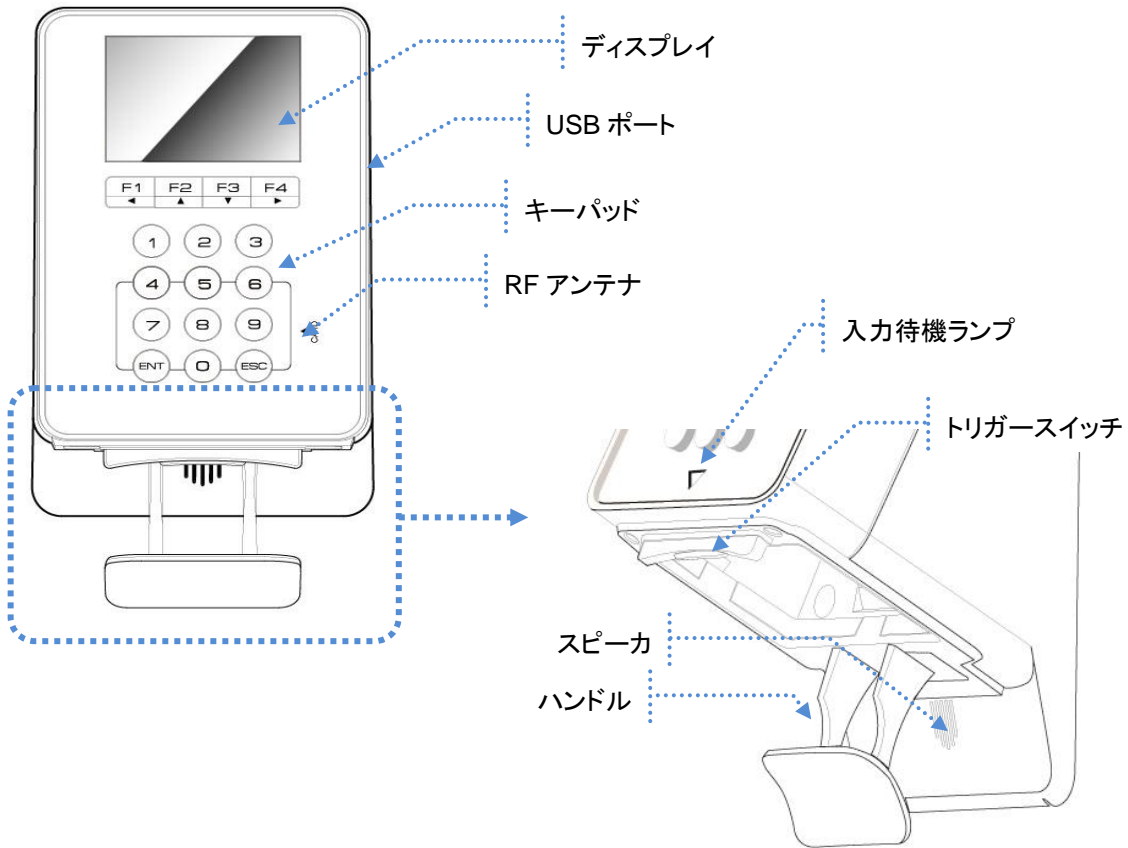
1. ファームウェアのアップグレード	48
2. 簡易設置説明書	50
2.1 VP-II Xの設置場所	50
2.2 ポートと接続	51
イベントレポートビューア(イベントログのバックアップ)	52
3.....	52
4. トレイアイコン.....	54

改訂情報

- V1 2009年5月26日 ドラフト
- V1.0 2009年6月3日 初版発行
- V1.2 2010年6月9日
 - － 関連するVP-II Xイメージをすべて変更
 - － ファームウェア(app-0.1.14.v56)の新規機能を追加
- V1.3 2011年10月25日
 - － 関連するVP-II Xイメージを一部変更
- V1.4 2012年3月22日
 - － P25「第3章 環境設定 1.2 マスタ/スレーブ設定 □DB同期機能とDB同期時間(マスタ)の説明追記。
 - － P26「第3章 環境設定 1.3 サーバ設定 □マスタのバックアップ機能の項目訂正および説明追記。項目変更 □ マスタのバックアップ機能 → □ バックアップマスタ機能
- V1.5 2015年5月15日
 - － ファームウェア(app-0.1.15.v32)の新規機能を追加
 - － P27「第3章 環境設定 2. システム設定 2.5 サマータイム、機能追加。
 - － P28「第3章 環境設定 2. システム設定 2.8 AUX設定 メニュー、機能追加。
 - － P29「第3章 環境設定 2. システム設定 2.9 1扉の入退認証モード。
 - － P38「第3章 環境設定 5. IC Card設定 5.3 ASI4000設定。
 - － P39「第3章 環境設定 5. IC Card設定 5.4 DUALI設定。
 - － P41「第3章 環境設定 6. ツール 6.1 DBバックアップ/リストア。
 - － P43「第3章 環境設定 6. ツール 6.3 ソフトリセット。

第 1 章 概要

1. VP-II X スキャナ



□ **ディスプレイ**
ステータスインジケータ



□ USB ポート

USB ポートは、ファームウェアのアップグレードまたはデータベースのバックアップ、リストアに使用します。

□ キーパッド

VP-II X のキーパッドは、テンキー(0~9)10 個、ENT キー(ENT)1 個、エスケープキー(ESC)1 個、機能キー(F1~F4)4 個から構成されています。機能キーは、パスワードの入力、勤怠管理に用いる場合の出勤／退勤の区別やジョブコードの転送、管理者メニューへのアクセスなど、特定の目的を持つ機能に使用されます。機能キーは、管理者メニューにアクセスしたときに矢印(方向)キーとしても使用されます。

□ 入力待機ランプ

使用者に手を入力するよう指示する LED です。

□ トリガースイッチ

使用者がこのスイッチを押すと、VP-II X は静脈データの取得を開始します。トリガースイッチは、入力待機 LED が点滅している場合のみ使用可能です。

□ スピーカー

VP-II X には、警告音や音声メッセージを流すためのスピーカーが内蔵されています。

□ ハンドル

使用者の手をスキャンに適した位置に固定するハンドルです。使用者は、指間の皮膜が触れるまで、2 つのガイドバーの間に中指を挿入する必要があります。

2. ネットワーク構成

VP-II X は、スタンドアロンとして構成することも、TCP/IP ネットワークを経由するネットワークシステムとして構成することもできます。ネットワーク環境で VP-II X を実行するには、適切なネットワークパラメータ設定が必要です。ネットワーク設定の詳細については、「第 3 章 1 ネットワーク設定」を参照してください。

2.1 マスタ／スレーブ運用

複数の VP-II X ユニットがネットワークに接続されている場合、そのうちの 1 台をマスタとして設定し、残りをスレーブとして設定する必要があります。VP-II X アプリケーションソフトウェア(NetControl-X)が実行されているサーバもマスタとして設定できます。この場合、VP-II X ユニットはすべてスレーブに設定されます。

□ マスタ

マスタユニットは、そのサイトにあるネットワークデータベースをすべて管理します。1 つのネットワークにつき、マスタは 1 つのみである必要があります。マスタは VP-II X でもサーバでもかまいませんが 1 つのネットワークで 64 を超えるユニットの VP-II X が動作している場合、VP-II X はマスタになれず、サーバをマスタとして動作させる必要があります。マスタとして設定されている VP-II X が対応できるスレーブは最大 63 ユニットです。

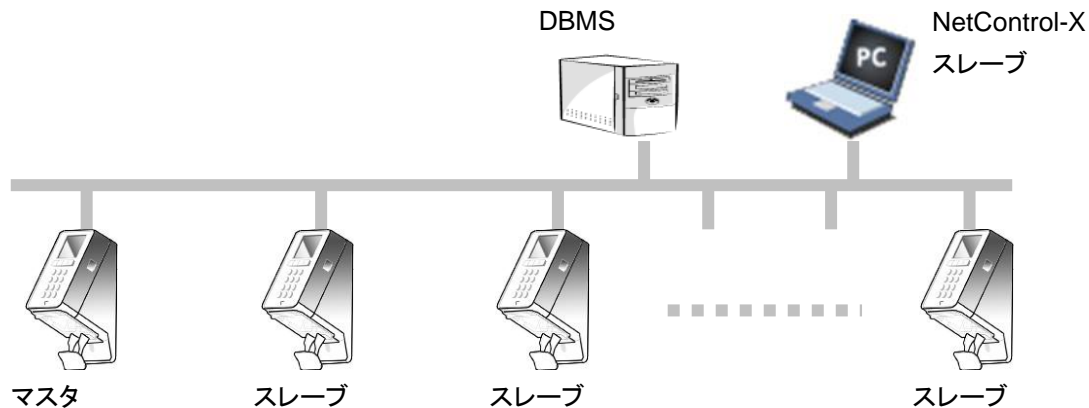
スタンドアロンとして動作する VP-II X はマスタに設定する必要があります。工場出荷時のデフォルトはマスタに設定されています。

□ スレーブ

スレーブユニットのデータベースは、マスタのデータベースと同期されます。管理者はスレーブでユーザーを登録または削除できますが、スレーブユニットは常にマスタのデータベースを参照するため、ユーザーを登録または削除するときにはマスタユニットが使用可能でなければなりません。ただし、認証は、マスタユニットのステータスに関係なく、いつでもスレーブユニットで実行できます。

2.2 ネットワーク設定

VP-II X ユニットは TCP/IP ネットワーク経由でネットワークに接続され、各ユニットのデータベースはすべて、自動的に同期されます。サーバなしでも最大 64 ユニットをネットワーク接続できますが、高度なユーザー管理、アンチパニック、イベントなど、VP-II X システムの強化された機能を活用するために、サーバで実行するアプリケーション ソフトウェア (NetControl-X) の使用をお勧めします。下の図は、複数の VP-II X ユニットとソフトウェア (NetControl-X) を使った一般的なネットワーク構成を示しています。



3. VP-II X の仕様

環境仕様	
電源電圧	DC 12V/1.5A (VP-II XGDコントローラまたはACアダプタより供給)
使用温度	-5~50°C
使用湿度	10% ~ 90%

物理仕様	
材質	スキャナ: PC + ABS 背面プレートおよびバックプレート: 金属
重量	820g(カードリーダーモジュール非搭載時)
寸法	109x247x117mm(詳細は図を参照)

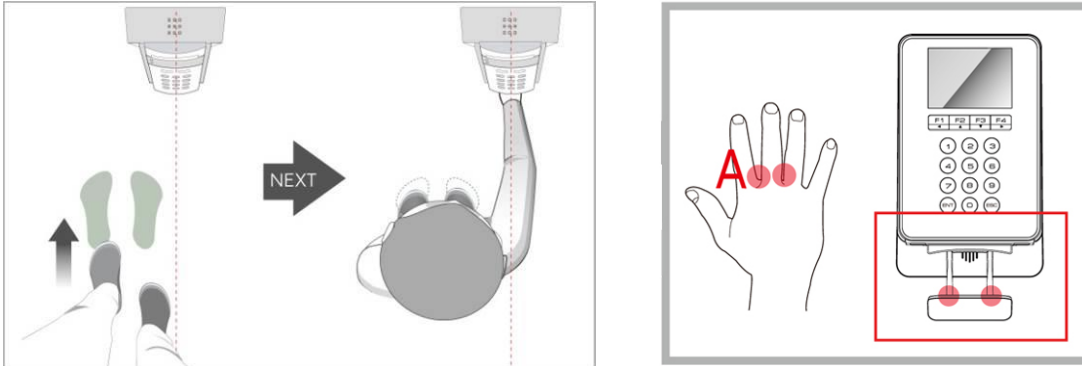
生体認証機能	
使用されるテクノロジー	人間の手の甲の静脈パターン認識 (HVPR)
精度	他人受入率 (FAR): 0.0001%以下 本人拒否率 (FRR): 0.01% レベルを 5 段階に変更可能: 1(最高精度)~5。レベルは使用者ごとまたは VP-II X ユニットごとに個別設定可能。
ユーザビリティ	99.98%(ユーザビリティ: 全人口に対して、システムを正しく使用できる使用者の割合)
速度	認証 1 回あたり 0.4 秒、登録には 0.4 秒×2 回
生体検知	生体識別 (HCD) アルゴリズム: 人間以外のものの登録は許可されない 設定可能レベル: 1(最も厳密)~3、または Off: 無効化 赤外線ベースのセンサ機器 非接触センサ 皮下からの生体認証機能(静脈データ) なりすましを回避 条件の厳しい環境に対する堅牢性 使用者のプライバシーを保護

ハードウェア仕様	
コアプロセッサ	Dual CPU(400MHz DSP、180MHz ARM プロセッサ)
表示画面	65K カラー2.8 インチ TFT 液晶(バックライト付き) 耐用年数:10 年間
キーパッド	0~9 キー、ENT キー、ESC キー、および機能キー4 個
外部インターフェース 入出力ポート	RJ45 イーサネット TCP/IP(VP-II X およびサーバと接続) Wiegand(入力:1、出力: 1) シリアルポート:2 チャンネル RS232 のみ: 1 RS232/RS485 共有:1(オプションの RS485 モジュールが必要) AUX: デジタル I/O(入力:2、出力: 2)
メモリ	512MB の NAND フラッシュメモリを内蔵 最大 5 万人の使用者のデータベース 最大 50 万件のログ(使用者のトランザクションやシステムイベント) ファームウェア、GUI、フォントなどの記憶域
USB 2.0	USB メモリ機器(ファームウェアのアップグレード、DB の転送) 管理者により承認された場合のみ利用可能 その他の用途:無線 LAN、外付けキーボード
カードモジュール	内蔵カードリーダーモジュール(オプション) 125KHz Prox カードリーダー 13.5MHz Mifare/DESFire/TWIC/PIV 13.5MHz HID iClass 上の 3 つのうち、1 つのみ設置可能 125KHz および 13.5MHz 対応の内蔵アンテナ
RTC(Real Time Clock)	時刻を正確に保つための自動調整機能
スピーカー	サウンド/音声のサポート
IR センサ	使用者の検出、スリープモードからの起動
タンパースイッチ	背面カバーに設置済み

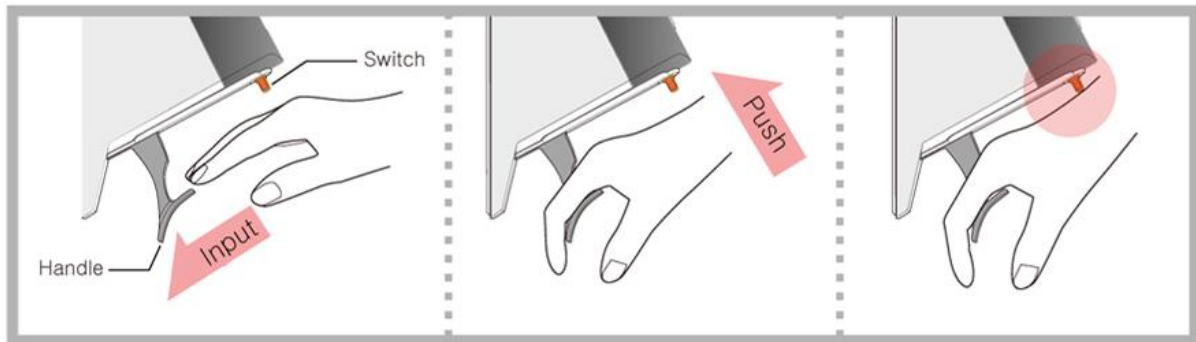
4. 手の入力についてのガイドライン

手の甲静脈パターンの認証パフォーマンスを最大限に高めるには、次の手順に従って、VP-II X スキャナに対して正しい位置に立ち、正しく手を置いてください。

- 腕をスキャナに向けてまっすぐ自然に伸ばせるように、スキャナの前の適切な位置に立ちます。たとえば、右手を使用する場合は、両足がスキャナの左側に来るように立ちます。



- 中指を 2 本のガイドバーの間に入れます。指間の皮膜が触れるまで、深く差し込んでください。その時に手を握らず、力を抜いて、ガイドバーの上に軽く乗せてください。



- 手首をトリガスイッチのほうにゆっくり持ち上げて、スイッチを押します。ハンドルを握らないでください。

誤った使い方

立ち位置が間違っています

ハンドルを握らないでください

指は奥まで入れてください

第 2 章 登録、削除、認証

1. 管理者メニュー

使用者の登録や削除、システム設定の変更には、管理者メニューへのアクセスが必要です。管理者メニューにアクセスできるのは、管理者またはインストーラだけです。納品時の VP-II X はテストモードに設定されています。このモードでは、インストーラを管理者として登録できます。

1.1 管理者

管理者は、使用者の登録と削除、システム設定のセットアップや変更を行う権利を持つ使用者です。管理者が認証されると、ディスプレイ上に管理者メニューが自動的に表示されます。

1.2 インストーラ

インストーラは、VP-II X がテストモードのときに登録できる一時的な管理者です。インストーラの権限は管理者と同じであり、管理者メニューにアクセスして、使用者の登録や削除、システム設定のセットアップや変更を行えます。通常、インストーラは設置時にシステムをセットアップするために、一時的に管理者として登録されます。設置が完了したら、インストーラを削除することをお勧めします。インストーラの登録で使用できるのは PIN のみで、カードは使用できませんが、管理者の登録にはカードと PIN の両方が使用できます。

1.3 テストモード

テストモードは、VP-II X の工場出荷時のデフォルト設定です。テストモードでは、VP-II X を起動するたびに、インストーラを管理者として登録するためのメニューが表示されます。つまり、ユニットがテストモードである限り、電源を入れなおせば誰でも管理者として登録できることになるため、いったん設置が完了したら、システム管理者がテストモードを解除することを強くお勧めします。

1.4 インストーラの登録

VP-II X がテストモードであるとき、起動のたびに、下のメニューが表示されます。インストーラ(システム管理者)を登録するには、ENT キーを押してから、表示される指示に従って PIN を入力し、手を 2 回入力します。インストーラの登録をスキップし、直接メイン画面に進むには、ESC キーを押します。

ユニット 1 つにつき、登録できるインストーラは 1 人だけです。同じユニットに新たにインストーラを登録すると、既存のインストーラは上書きされます。ただし、同一のネットワークに複数のユニットがある場合、ユニットごとに異なる PIN を持つ異なるインストーラを登録できます。



1.5 管理者メニューへのアクセス

使用者管理(登録、削除、変更)およびシステム設定を実行するには、管理者またはインストーラとして認証して、管理者メニューにアクセスする必要があります。管理者/インストーラの認証については、「第2章 4 認証」を参照してください。

1.6 管理者メニューの主な使い方

管理者メニューでは、カーソルを移動し項目を選択するための矢印キーとして、機能キーを使用します。ENTキーは、メニュー項目の選択や設定の保存のための決定キーとして使用されます。また、ESC キーは、メニューの終了や設定のキャンセルのために使用されます。メニューに番号が振られている場合は、テンキーを直接押して、メニューを選択することもできます。

1.7 メニューツリー

VP-II X管理者メニュー

1. 使用者管理	1. 使用者の登録 2. 使用者の削除 3. 使用者の変更 4. 静脈データ管理 5. インストーラの削除 6. IC カード更新	
2. 運用設定	1. モード設定 2. テストモード 3. キーパッド入力設定 4. スリープモード 5. タンパースイッチ設定 6. DB 検索オプション 7. 勤怠管理設定	
3. システム設定	1. ネットワーク設定	1. ネットワーク環境 2. マスタ/スレーブ設定 3. サーバ設定 4. スレーブリスト
	2. 日付/時刻設定	1. 日付/時刻設定 2. NTP TimeServer

	<ul style="list-style-type: none"> 3. ファームウェア情報 4. VP 設定 5. ドア設定 6. サマータイム 7. システム初期化 8. 施錠検知設定 9. AUX 設定 10. 1 扉の入退認証モード 	
4. UI 設定	<ul style="list-style-type: none"> 1. 言語設定 2. サウンド設定 3. PIN 表示オプション 4. 時計選択 	
5. IC Card 設定	<ul style="list-style-type: none"> 1. Wiegand 設定 2. Mifare カード 3. HID iClass カード 4. ASI4000 設定 5. DUALI 設定 6. PACS 設定 7. 入力設定 	
6. ツール	1. DB バックアップ/リストア	<ul style="list-style-type: none"> 1. DB バックアップ 2. DB リストア 3. イベントログのバックアップ
	2. 診断ツール	<ul style="list-style-type: none"> 1. ネットワーク診断 2. ネットワーク情報
	3. ソフトリセット	

2. 登録

使用者または管理者の登録には、管理者メニューまたは NetControl-X アプリケーションソフトウェアを使用します。使用者や管理者を登録するためには、管理者メニューへのアクセスが必要です。NetControl-X アプリケーションソフトウェアを使用した登録方法の詳細については、NetControl-X の取扱説明書を参照してください。

2.1 使用者タイプ

登録と認証に使用される ID 番号によって、使用者タイプが異なります。使用者や管理者は、PIN、HID Prox カード、IC カード、またはパスワードを使って登録できます。

□ PIN 使用者

2～24 桁の使用者番号 (PIN) を使用して登録された使用者。

□ HID Prox カード使用者

HID Prox カードを使用して登録された使用者。カードの Wiegand コードが PIN として使用されます。

□ IC カード使用者

IC カード (Mifare、DESFire、PIV/TWIC など) を使用して登録された使用者。この場合、静脈データはカードやサーバに保存されます。

□ パスワード使用者

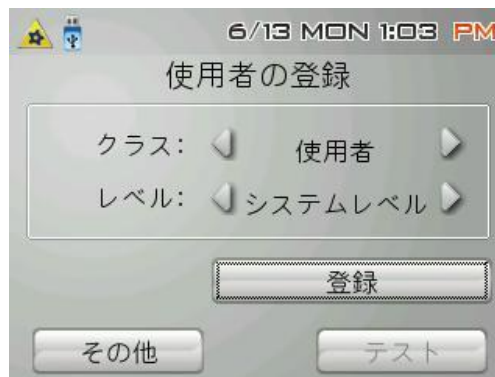
パスワードを使用して登録された使用者。認証時に静脈データが使用されません。キーパッドを使用してパスワードを入力するため、特別な手順が必要です。詳細については、「第 2 章 4.2 パスワード使用者の認証」を参照してください。

2.2 使用者／管理者の登録

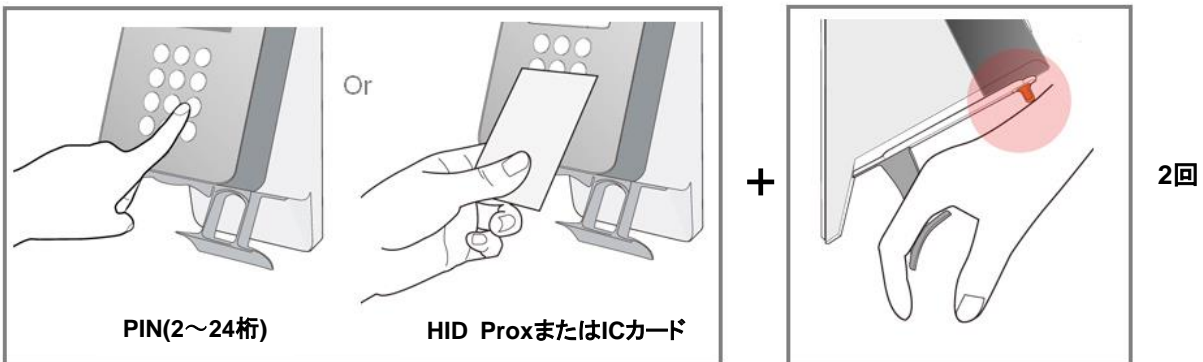
スレーブユニットで使用者を登録する場合、マスタユニットが動作している必要があります。スレーブがネットワーク上のマスタにアクセスできない場合、登録機能は使えません。使用者データは、いずれかのユニットでいったん登録が完了すれば、自動的に、ネットワーク上のすべてのユニットに配信されます。

使用者、または管理者を登録するには、管理者メニューにアクセスし、次のようにメニューを選択します。

管理者メニュー > 1. 使用者管理 > 1. 使用者の登録



クラスとレベルの設定後、またはデフォルトの設定(使用者とシステムレベル)をそのまま使用して、[登録]を実行して登録プロセスを開始します。その後、表示画面に表示される手順に従って操作します。最初に、PIN(2～24桁)の入力またはカード(HID ProxカードかICカード)の提示を行います。その後、手を入力します。入力されたPINと静脈データが正しいことを確認するために、このプロセスは2回行う必要があります。



2.2.1 登録オプション

□ クラス

[使用者]または[管理者]を選択して登録します。複数の管理者を登録できます。

□ レベル(セキュリティレベル)

登録する使用者に個人のセキュリティレベルを割り当てるには、1～5 からレベルを選択します。[システムレベル]を選択すると、ユニットで設定されるレベルが使用されます。VP-II X に最初に登録する使用者については、デフォルトの[システムレベル]を使用することをお勧めします。また、NetControl-X および VP-II X の管理者メ

ニューを使用して、個人のセキュリティレベルを変更することができます。詳細は、「第 2 章 5.1 使用者の情報設定」を参照してください。

このレベルは、認証のために静脈の生体認証データを照合する際に使用される、調節可能なセキュリティレベルを示しています。レベルは 5 段階に調節できます。レベル 1 では、最も厳密に静脈データの照合が行われます。高いレベル 1 では照合の精度が高くなりますが、個人の静脈データの特性や環境によっては、本人拒否率も高くなる可能性があります。

工場出荷時のデフォルト設定はレベル 3 です。初めての導入では、使用者に立ち位置やスキャナに手を入力する方法をトレーニングするため、このレベルの使用をお勧めします。導入とトレーニングが完了したら、VP-II X のシステムレベルをレベル 3 以上に設定することをお勧めします。個人のセキュリティレベルは、固有の要件に基づいて、使用者ごとに調節することができます。

VP-II X ユニットにはそれぞれセキュリティレベル(システムレベル)が設定されています。これは、各使用者のセキュリティレベル(個人のセキュリティレベル)として指定することができます。使用者を認証する場合、VP-II X は、個人のセキュリティレベルが指定されている場合はそのレベルを、指定されていない場合はシステムレベルを使用します。

□ テスト

登録が適切に行われたかどうかを確認するには、この機能を使用します。[テスト]を実行すると、認証プロセスが開始され、使用者が認証のテストすることができます。使用者を適切に認証できない場合は、再登録してください。

□ その他

下に示す追加オプションが表示されます。これにより、使用者の開始時刻や有効期限を有効化することができます。[有効]を選択し、開始時刻や有効期限を設定します。開始時刻を設定した場合、使用者はその日時までアクセスできません。このオプションは、NetControl-X ソフトウェアでも設定できます。

6/13 MON 1:04 PM

使用者の登録

開始時刻 : 有効

年 月 日 時 分

2011 6 13 13 4

有効期限 : 有効

年 月 日 時 分

2011 6 13 13 4

パスワード : 有効

□ パスワード

これは、静脈データを登録せずに、4~10 桁のパスワードだけを使って使用者を登録するためのオプションです。パスワードが割り当てられている場合、PIN またはカードに続けて、パスワードを入力するだけで、アクセスできます。パスワードを使用してアクセスする方法の詳細については、「第 2 章 4.2 パスワード使用者の認証」を参照してください。

3. 削除

管理者は、管理者メニューから使用者を削除できます。スレーブユニットから使用者を削除する場合、マスタユニットが動作しており、スレーブユニットがマスタユニットのデータベースにアクセスできる必要があります。あるユニットで使用者を削除すると、ネットワークにあるすべてのユニットのデータベースから、この使用者のデータが自動的に削除されます。

3.1 インストーラの削除

設置が完了したら、管理者と同じ権利を持つインストーラを管理者が削除することを強くお勧めします。インストーラを削除するには、次のようにメニューを選択します。

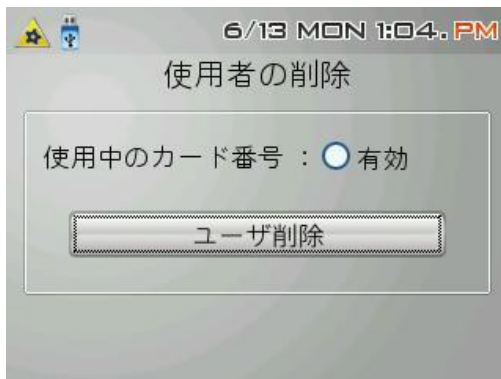
VP-II X からインストーラを削除する場合、そのユニットに登録されているインストーラのみが削除されます。つまり、ネットワーク上の他のユニットに登録されたインストーラの PIN はそのまま残ります。同じネットワーク上にあるユニットすべてのインストーラの PIN を削除するには、NetControl-X ソフトウェアを使用します。

管理者メニュー > 1. 使用者管理 > 5. インストーラの削除

3.2 使用者の削除

管理者メニュー > 1. 使用者管理 > 2. 使用者の削除

□ 使用者の削除



この機能では 1 人の使用者を削除します。削除する使用者の PIN を入力するか、カードを提示します。表示される手順に従って、削除を完了してください。

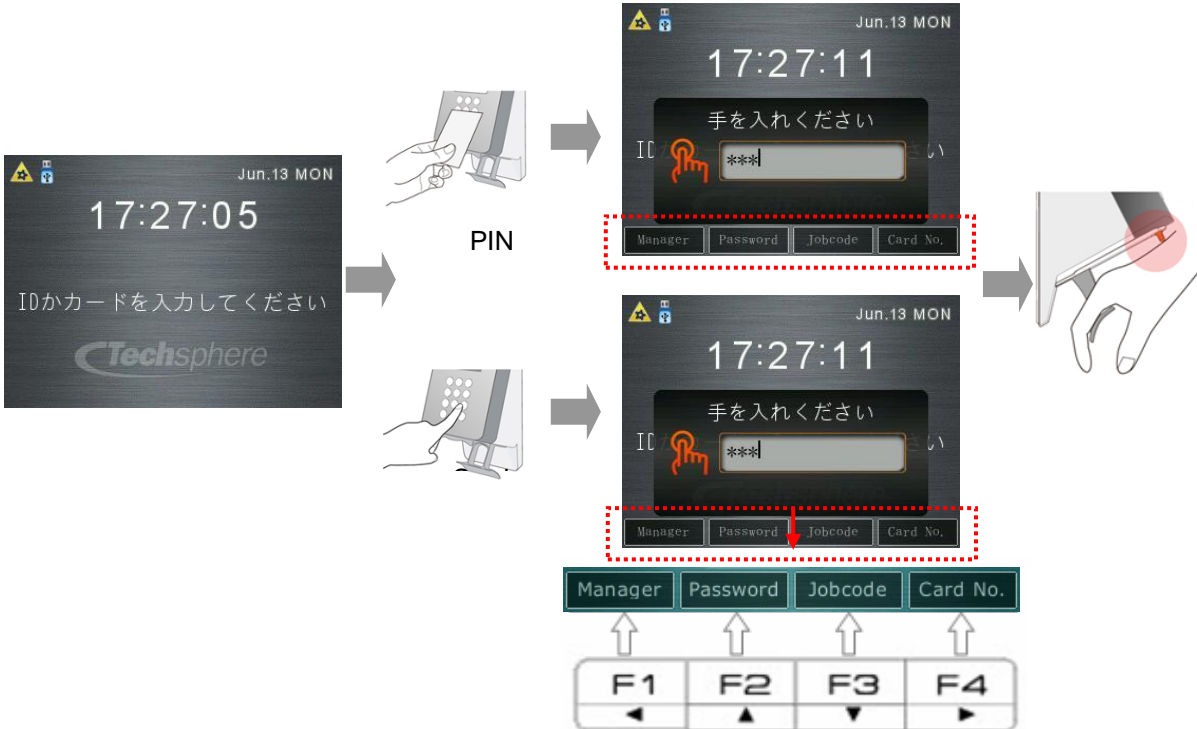
削除できる対象は使用者だけです。このメニューから直接、管理者を削除することはできません。管理者を削除するには、使用者クラスを[使用者]に変更する必要があります。管理者の使用者クラスを[使用者]に変更する手順については、「第 2 章 5.1 使用者の情報設定」を参照してください。

□ 使用中のカード番号

カード使用者を削除する場合、Wiegand PIN が有効化されていれば、Wiegand PIN を使用して削除します。VP-II X は、カード番号を使用して、カード使用者を削除します。カード番号を正確に照合するために、VP-II X をシステムで適切な Wiegand 形式に設定する必要があります。カード使用者に対して Wiegand 形式を設定する手順については、「第 3 章 5.1 Wiegand 設定」を参照してください。

4. 認証

認証は通常、(1)PIN を入力するかカードを提示し、(2)手を入力して行われます。



PIN を入力するかカードを提示すると、上の図に示すように、画面の下部にサブメニューが表示されます。使用者または管理者は、次の選択肢から選択できます。F1 は管理者、F2 はパスワード認証、F3 は勤怠用ジョブコード、F4 は使用者がカードを提示する代わりにカード番号を入力します。目的の操作に対応した F キーを選択します。これ以降の手順を参照してください。

4.1 管理者の認証

管理者認証を受けるには、(1)管理者の PIN を入力するか管理者のカードを提示し、(2)F1 キーを押して管理者の認証に進み、(3)手を入力します。下の図は、PIN 入力を使用した管理者認証の例を示しています。



管理者が認証されると、自動的に管理者メニューが表示されます。

注意: 管理者が認証されたとき、VP-II X は、Wiegand 出力や解錠信号を送信しません。

4.2 パスワード使用者の認証

パスワード使用者は、手の甲の静脈パターンを使用して認証を受ける必要はありません。パスワード使用者は、PIN またはカードと、登録時に割り当てられたパスワードだけで入退室できます。

パスワード使用者が認証するには、(1) PIN を入力するかカードを提示し、(2) F2 を押してパスワードの入力に進み、(3) 手を入力し、トリガースイッチを押します (VP-II X による手の認証は行われませんが、使用者はスイッチに手を入れる必要があります)。

4.3 ジョブコードの入力

VP-II X を勤怠管理に使用しているときに、ジョブコードの入力が必要である場合、使用者は手の認証の前にジョブコードを入力できます。ジョブコードに使用できるのは数字だけです (例: 1234, 20000, 6666666)。

ジョブコードを入力するには、(1) PIN を入力するかカードを提示し、(2) F3 キーを押してジョブコードの入力に進み、(3) 手を入力します。

4.4 カード番号を使った認証

この機能を使用すると、HID Prox カード使用者は、カードを提示する代わりにカード番号を直接入力することができます。この機能を使用するには、あらかじめ、適切な Wiegand 形式 (パリティビット、サイトコード、カードのシリアル番号のビット長) を設定しておく必要があります。Wiegand 形式の設定方法の詳細については、「第 3 章 5.1 Wiegand 設定」を参照してください。

カード番号を使って認証を受けるには、(1) キーパッドを使用してカード番号を入力し、(2) F4 キーを押してカード番号の認証に進み、(3) 手を入力します。

4.5 機能キーを使った認証

機能キーは通常、勤怠管理の目的で使用されます。機能キーを使用する場合、使用者は PIN の入力やカードの提示の前に機能キーを押す必要があります。

(1) 機能キー (F1~F4) を押す (2) PIN を入力またはカードを提示する (3) 手を入力する

VP-II X は、使用者トランザクションイベントとともに、機能キー情報 (なし、F1、F2、F3、F4 のいずれか) を NetControl-X ソフトウェアに送信します。各機能キーの用途 (たとえば、F1 は出勤、F2 は退勤など) は、NetControl-X で割り当てられます。

より高度な勤怠管理用途のために、機能キーをカスタマイズして、複数レベルのジョブコードを転送したり、個別の出退勤を表示したりすることができます。

4.6 脅迫警報コードを使った認証

VP-II X には、使用者がアクセスを強要された場合に警報を生成できる機能があります。脅迫警報コードの生成方法は 2 つあります。

1 つめの方法では、PIN の入力またはカードの提示の前に、ENT キーを押します。警報を生成するには、(1) ENT キーを押し、(2) PIN を入力するかカードを提示し、(3) 手を入力します。

2 つめの方法では、使用者の両手を登録し、どちらかの手を脅迫認証／通知に使用します。XP-II X では、使用者は両手を登録できます。1 人の使用者が両手を登録する方法の詳細は、「5.2.2 複数のテンプレートの割り当て」を参照してください。また、脅迫認証に使用する手の割り当て方法については、「5.1 使用者の情報設定」を参照してください。

脅迫認証が行われた場合、VP-II X は次の 3 つの方法で警報イベントを送信できます。1)リアルタイムで警報イベントを NetControl-X ソフトウェアに送信し、NetControl-X は警報メッセージを生成して、あらかじめ指定されたアカウントに電子メールを送信する。2) 必要に応じてファームウェアを変更することで、VP-II X からデジタル信号を AUX ポート経由で送信する。3) 他入退室管理システムに事前定義されている Wiegand サイトコードを送信する(Wiegand オプションの設定の詳細については、「3 5.1.3 Wiegand の出力オプション」を参照)。この機能については、販売店にお問い合わせください。

4.7 インストーラの認証

インストーラが認証するには、(1)ENT キーを 2 回押し、(2)インストーラの PIN を入力し、(3)手を入力します。ENT キーを 2 回押しと、下の図にあるように、インストーラの認証を示すメッセージが PIN 入力欄の上に表示されます。**注意: インストーラの認証時には、Wiegand 出力や解錠信号は出力されません。**



5. 使用者情報の変更

5.1 使用者の変更

登録済み使用者の使用者情報を変更するには、この機能を使用します。使用者の情報を変更するには、次のようにメニューを選択します。

管理者メニュー > 1. 使用者管理 > 3. 使用者の変更

次のウィンドウが表示されたら、XP-II X に PIN を入力するか使用者のカードを提示して、変更する使用者データを取得します。この機能を実行する場合、ネットワーク上のすべてのユニットで使用者情報を更新できるように、マスタユニットが動作している必要があります。

IC カードの使用者には、この機能は使用できません。IC カード使用者は、いったん削除してから、再登録する必要があります。



□ クラス/レベル

使用者クラス([管理者]または[使用者])およびセキュリティレベル(個人レベル 1~5 または[システムレベル])は再割り当てできます。

□ 脅迫

脅迫認証に使用する手(静脈データ)を選択します。この機能は、1 人の使用者が両手を登録している場合のみ使用可能です。ここで選択した手で使用者が認証された場合、それは脅迫認証であると見なされ、ドアまたはゲートが開かれますが、警報が自動的に発生します。脅迫認証の詳細については、「4.6 脅迫警報コードを使った認証」を参照してください。

通常のアクセスを行うための認証には、ここで選択していないほうの手を使用する必要があります。

□ 有効/無効

これはシステムからデータを削除せずに使用者を無効化する機能です。無効化された使用者はアクセスできなくなりますが、この使用者のデータはシステムデータベースに残っていますので再登録せずに、このメニューを使って有効化することができます。

□ 開始時刻と有効期限

開始時刻を設定した場合、使用者はその日時までアクセスできません。デフォルトでは、開始時刻が指定されていない場合、すべての使用者は登録と同時にシステムの使用が許可されます。

同様に、有効期限が設定されている場合、この日時が過ぎると、使用者のデータがデータベースに存在していても、この使用者はシステムにアクセスできません。

□ パスワード

選択した使用者に対してパスワードを割り当てるための機能です。パスワードが割り当てられている場合、使用者は、PIN またはカードに続けてパスワードを入力するだけでアクセスを得られます。パスワード使用者については、手の甲静脈認証は必要ありません。パスワード使用者の認証の詳細については、「4.2 パスワード使用者の認証」を参照してください。

5.2 静脈データ管理(静脈データの追加/再登録)

5.2.1 静脈データの更新

登録済み使用者の静脈データは、NetControl-X データベースの使用者情報を変更せずに更新することができます。これにより、登録が適切に行われていないかトレーニングが足りないために認証が難しい既存の使用者のみの静脈データを再登録し、更新することができます。この場合、使用者名や有効期限などの既存の情報を再登録する必要はありません。これらの情報はデータベースに保持されます。

IC カードの使用者には、この機能は使用できません。IC カード使用者が静脈データを更新する方法については、「5.2.3 IC カード更新」を参照してください。

5.2.2 複数のテンプレートの割り当て

1 人の使用者はテンプレートを 2 つまで持つことができます。この機能により、使用者は、右手と左手の両方を登録するか、どちらかの手を 2 回登録できます。

この機能は同じ手を別の時期に 2 回登録するために使用できます。たとえば、冬に 1 回、夏に 1 回登録して、暑さや寒さなどの気候条件による、抽出された静脈パターンのわずかな変化を原因とする本人拒否率を最小限に抑えることができます。また、2 つめのテンプレートを脅迫認証に使用することもできます。脅迫認証の詳細については、「4.6 脅迫警報コードを使った認証」を参照してください。

下のようにメニューを選択します。

管理者メニュー > 1. 使用者管理 > 4. 静脈データ管理

メニューの選択後、処理の対象となる使用者の PIN を入力するか、カードを提示します。この機能をスレーブユニットで実行する場合は、マスタユニットが動作している必要があります。ネットワーク上のマスタユニットに接続できない場合、スレーブユニットがマスタ上のデータベースで使用者データを更新できないため、この機能は使用できません。



テンプレート番号は、登録されている静脈データ(テンプレート)の数を示します。つまり、「1」だけがマークされている場合、テンプレートが 1 つしか登録されていません。テンプレートが 2 つ登録されている場合は、「1」と「2」の両方がマークされます。

テンプレートが 1 つだけ登録されている(テンプレート番号「1」だけがマークされている)ときに、2 つめのテンプレートを登録するには、[削除/追加/再登録する PIN を選んで下さい]で[2]を選択し、[追加/再登録]を実行します。これにより、2 つめのテンプレートが自動的に登録されます。

静脈データを更新するには、テンプレート番号 1 または 2(登録されている場合)を選択し、[追加/再登録]を実行します。2 つめのテンプレートを削除するには、テンプレート番号 2 を選択して、[削除]を実行します(このメニューではテンプレート番号 1 は削除できません。[使用者の削除]メニューを使用して、使用者を削除してください)。

5.2.3 IC カード更新

IC カードの使用者は、このメニューを使用して静脈データを更新することができます。管理者メニューから[1. 使用者の管理]を選択し、[6. IC カード更新]を選択します。

管理者メニュー > 1. 使用者管理 > 6. IC カード更新



第3章 環境設定

1. ネットワーク設定

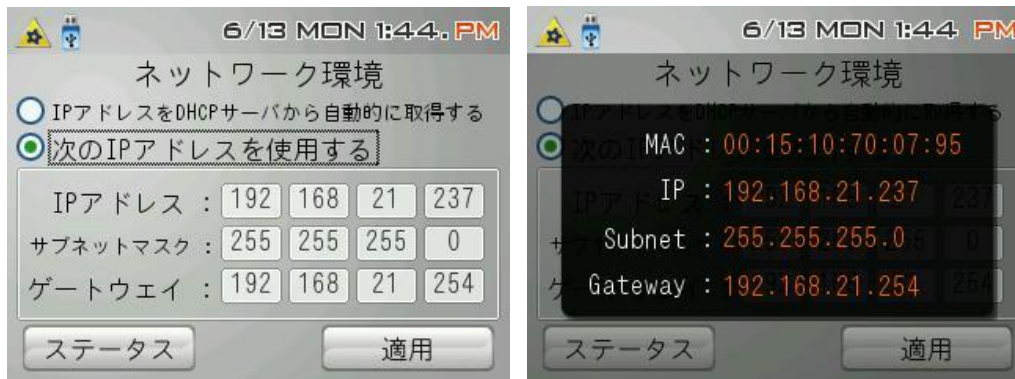
TCP/IP ネットワーク環境で VP-II X を動作させるには、適切なネットワーク環境設定が必要です。IP アドレス（サブネットマスクとゲートウェイを含む）、マスタ IP アドレス、サーバ IP アドレス（使用している場合）、およびスレーブ情報（マスタユニットのみ）を設定する必要があります。詳細は、以下のセクションを参照してください。

1.1 ネットワーク環境の設定(TCP/IP パラメータ)

すべての VP-II X は、ネットワークで使用するためには、IP アドレスが必要であり、TCP/IP ネットワークパラメータを適切に設定する必要があります。

管理者メニュー > 3. システム設定 > 1. ネットワーク設定 > 1. ネットワーク環境

サイトのネットワーク環境によって、VP-II X が DHCP サーバから自動的に IP アドレスを取得することも、管理者が手動で IP アドレスを割り当てることもできます。IP アドレスを手動で設定する場合は、すべてのネットワークパラメータが適切に設定されていることと、ネットワークで IP が競合していないことを確認してください。また、サーバから ping コマンドを使用して、TCP/IP 通信ステータスをテストすることを強くお勧めします。



□ ステータス

これは、現在設定されているネットワークパラメータ(IP アドレス、サブネットマスク、およびゲートウェイ)を表示します。IP アドレスが適切に設定されていない場合、IP アドレス 128.0.0.1(工場出荷時のデフォルト値)が表示されます。

1.2 マスタ/スレーブ設定

1 台の VP-II X をマスタに設定し、ネットワークにある残りの VP-II X をスレーブに設定する必要があります。ネットワークでの運用の詳細については、「2 ネットワーク構成」を参照してください。

マスタ/スレーブを設定し、マスタ/スレーブ運用に必要なパラメータを設定するには、次のようにメニューを選択します。

管理者メニュー > 3. システム設定 > 1. ネットワーク設定 > 2. マスタ/スレーブ設定

マスタモードまたはスレーブモードを選択します。スレーブモードを選択した場合は、マスタ IP を設定する必要があります。マスタモードを選択した場合は、マスタ IP は必要ありません。1 つのネットワークにマスタユニットが 1 つだけ存在することを確認してください。

サーバ(NetControl-X)がマスタに設定されている場合、すべての VP-II X ユニートをスレーブに設定する必要があります。この場合、サーバの IP アドレスをマスタ IP として入力する必要があります。

□ ポート

デフォルトポート(61235)がすでに使用されている場合や別のシステム用に予約されている場合は、VP-II X システムで使用される TCP/IP ポートを変更できます。ポート番号には 60000 よりも大きな値を使用することをお勧めします。ネットワークにあるすべての VP-II X ユニートおよびサーバに同じポート番号を適用する必要があります。

□ DB 同期機能と DB 同期時間(マスタ)

マスタは定期的にはスレーブのデータベースを監視し、マスタ内のデータベースと同期します。これにより、スレーブのデータベースがマスタのデータベースと同期され、すべてのスレーブで、ネットワークに接続していなくても認証を行えるようになります。またスレーブユニット上に使用者情報と静脈データを格納することが望ましくない用途では、DB 同期機能を無効にする必要があります。これにより、スレーブユニットがユニット上に使用者情報を格納することはなくなります。DB 同期機能無効時に静脈パターンを認証する場合、使用者が手をスレーブユニットに入力すると、スレーブユニットは登録された静脈データが格納されているマスタ VP-II X またはサーバと通信し、手を認証します。認証場所を[ネットワークのみ]に設定する手順については、「第 3 章 3.6」を参照してください。

またマスタは、ここで設定された間隔(分)でこの操作を実行します。同期時間の範囲は 20~1440 分(24 時間)です。

□ ハートビート時間(スレーブ)

ハートビートは、通信ステータスを確認するためのスレーブとマスタ間の通信プロトコルです。スレーブはマスタにハートビートプロトコルを送出し、ここで設定されている時間(秒)内の応答をチェックします。ハートビート時間の範囲は 10~255 秒です。

1.3 サーバ設定

NetControl-X を使用している場合、NetControl-X が実行されているサーバの IP アドレスを、ネットワーク上の各 VP-II X ユニットで設定する必要があります。

管理者メニュー > 3. システム設定 > 1. ネットワーク設定 > 3. サーバ設定

サーバ IP、ポート、ハートビート時間を、前のセクションで説明したマスタ/スレーブと同じ方法で設定します。

□ バックアップマスタ機能

マスタユニットとの通信が切断された場合にスレーブユニットはサーバ PC をマスタユニットとして認証操作することが出来ます。(ただし登録および削除操作は出来ません)

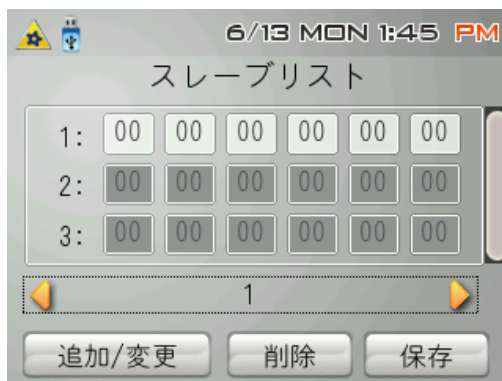
※バックアップマスタ機能を使用する場合は以下の設定および条件が必要となりますのでご注意ください。

- ・マスタ/スレーブ設定でマスタユニットの DB 同期機能を無効にする。(「1.2 マスタ/スレーブ設定 □ DB 同期機能と DB 同期時間(マスタ)」を参照してください。)
- ・サーバ設定でバックアップマスタ機能を有効にする。
- ・DB 検索オプションで 1st:Network, 2nd:Local, Only Network のいずれかを選択する。(3.6 DB 検索オプションを参照してください。)
- ・サーバ PC および管理アプリケーション NetControl-X の使用(インストールおよびセットアップ。)

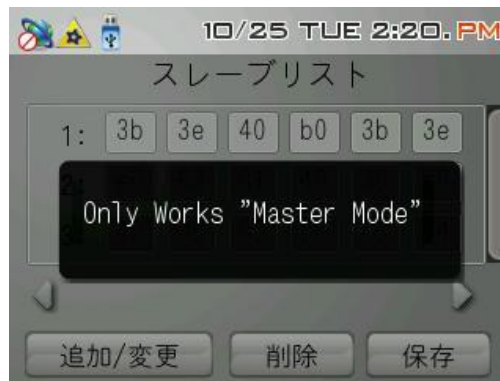
1.4 スレーブリスト

この機能は、マスタユニットでのみ使用できます。マスタにより管理されているスレーブのリストを確認、追加、削除できます。このリストでは、MAC アドレスが使用されます。スレーブリストは、XConfig ソフトウェアを使用して設定した場合自動的に作成されます。また、このメニューから手動で設定することもできます。

管理者メニュー > 13. システム設定 > 1. ネットワーク設定 > 4. スレーブリスト



マスタユニットでの表示画面



スレーブユニットでの表示画面

2. システム設定

2.1 日付／時刻設定

ユニットの日付と時刻は次のメニューで設定できます。日付と時刻はマスタとスレーブの両方で設定できますが、スレーブの日付と時刻は、定期的にマスタの日付と時刻に自動的に同期されます。

管理者メニュー > 3. システム設定 > 2. 日付／時刻設定

2.2 ファームウェア情報

これは VP-II X のファームウェア情報を示します。使用されているファームウェアファイルには、Boot、Kernel、Ramdisk、Application、Media の 5 種類があります。

管理者メニュー > 3. システム設定 > 3. ファームウェア情報



□ USB 検索(ファームウェアアップグレード)

USB メモリスティックを使用してファームウェアをアップグレードすることができます。USB ドライブで、下に示すようなフォルダを作成し、このフォルダにファームウェアを置きます。その後、VP-II X の USB ポート(「1 VP-II X スキャナ」を参照)に USB 機器を差し込み、[USB 検索]を実行します。これにより、ファームウェアが自動的に検索され、可能であれば、アップグレードが行われます。

USB Driver:¥Techsphere¥VP-IIX¥Firmware¥

ファームウェアは上に示すフォルダに入っている必要があります。そうでない場合、VP-II X は、ファームウェアを見つけてアップグレードを実行することができません。

2.3 VP 設定(セキュリティレベル、生体検知、認証試行回数)

システムのセキュリティレベル、生体識別機能(HCD)レベル、試行回数を設定または変更するには、次のようにメニューを選択します。

管理者メニュー > 3. システム設定 > 4. VP 設定

□ システムレベル

使用者の認証に使用されるシステムセキュリティレベル(1~5)を設定します。セキュリティレベルについては、「2.2.1 登録オプション」の「レベル(セキュリティレベル)」を参照してください。このメニューは、システムのセキュリティレベルを設定するためのものです。個人のセキュリティレベルは、登録時に、または[使用者の情報設定]メニューを使って、個別に設定できます(「5.1 使用者の情報設定」を参照)。

□ HCD レベル

VP-II X が採用している静脈パターン認証テクノロジーは、人間か人間ではない物体かを認識できます。このメニューでは、その判断レベルを調節できます。範囲は 1(最も厳密)~3、またはオフ(無効)です。

レベル 1:HCD が、最も厳密なレベルで、登録と認証の両方に適用されます。このレベルでは、人間の手のみを登録および認証できます。

レベル 2 および 3:HCD は登録にのみ適用され、認証には適用されません。オフ:HCD 機能は使用されません。

□ 認証試行回数

手の認証に失敗したときの再試行回数を 2~5 回の範囲で設定します。デフォルト値は 2 回です。

2.4 ドア設定

VP-II X システムは、PACS(他入退室管理システム)を使用せずに、コントローラからドアを制御できます。ドアの制御に必要なパラメータの設定および変更には、次のメニューを使用します。

管理者メニュー > 3. システム設定 > 5. ドア設定



- コントローラドアの制御に使用するコントローラを選択します。コントローラとして VP-II XG が選択されていますが、他のコントローラオプションも、使用可能になり次第追加される予定です。コントローラを使用しない場合は、[None]を選択します。

2.4.1 VP-II XG(ドアコントローラ)

VP-II X は、VP-II XG ドアコントローラを通じて、電気錠を制御できます。VP-II XG は別供給で、RS232 または RS485 経由で VP-II X に接続します(RS485 インターフェースを使用するには、VP-II X と XG の両方にオプションの RS485 ドライバボードを設置する必要があります)。VP-II XG には、電気錠に接続するためのリレー出力と、ドアステータスの監視および解錠入力インターフェース用デジタル入力ポートがあります。

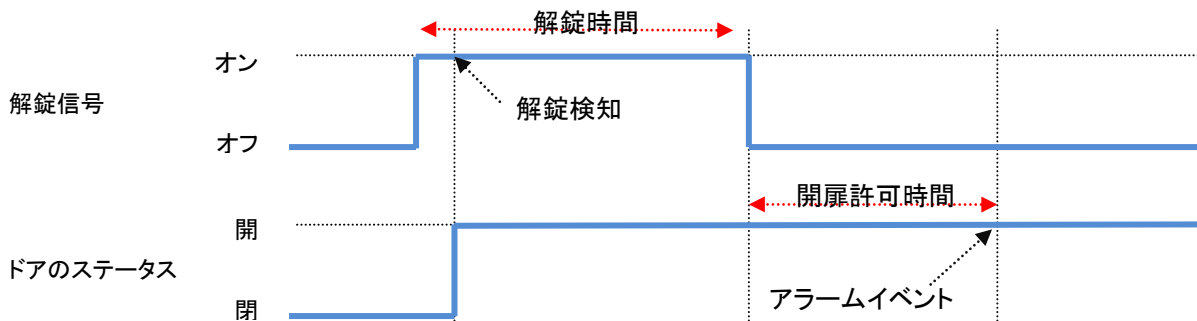
□ 解錠時間

これは、ドアの解錠信号が有効な時間を設定します。1~255 秒の範囲で設定できます。使用者が正しく認証されると、VP-II XG はリレーに解錠信号を出力し、ここで設定された時間、信号を維持します。

□ 開扉許可時間

開扉許可時間とは、VP-II XG が解錠信号を解除した時点からドアを開けたままにしておくことができる最大時間を意味します。範囲は 1~255 秒です。

この機能を使用するには、施錠検知センサが使用可能であり、VP-II X のドアモニタリング入力ポートに接続されている必要があります。VP-II X はドアモニタリング入力ポートを通じて、ドアが開いているか閉じているかといったドアのステータスを監視し、開扉許可時間内にドアが閉じられなかった場合は、イベントアラームを生成します。



□ 機能キー(解錠)

これは、機能キーを入力した使用者が認証されたときに、VP-II X が解錠信号を生成するかどうかを決定します。各機能キーを必要に応じて選択または選択解除してください。

たとえば、このメニューで F1 の選択を無効にした場合、使用者が PIN を入力する前に F1 を押すと、VP-II X はこの使用者の認証が成功しても解錠しません。

このオプションは、勤怠管理において、機能キーを使用して出勤や退勤を認証しているときにドアを解錠することが望ましくない用途のための機能です。

□ ペアリング

セキュリティ上の理由から、ある VP-II X 機器にどの XG 機器の接続を許可するかを制御する必要があります。ペアリングされている機器の片方を交換した場合、もう一度、ペアリングし直す必要があります。それまでは、VP-II X と XG 機器は互いに通信できません。

2.5 サマータイム

サマータイムを採用している地域では、サマータイムの開始日時や終了日時を設定することで、VP-II X の時刻が調整されるように設定することができます。いったん設定すれば、VP-II X の時刻は、設定された日時に基づいて自動的に調整されます。下の図は、タイプ設定を設定するメニューを示しています。

Type 1: 週、曜日、月、時、分 Type 2: 月、日、時、分

管理者メニュー > 3. システム設定 > 6. サマータイム【デフォルト値: Disable(無効)】



2.6 システム初期化(工場出荷設定にリセット)

システム設定をすべて工場出荷設定にリセットすることができます。

注意: この機能を実行するときは、特に注意を払う必要があります。

管理者メニュー > 3. システム設定 > 7. システム初期化

□ 設定初期化

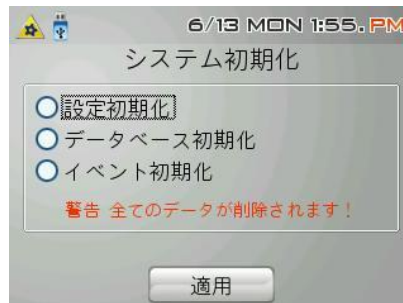
これにより、すべての設定が工場出荷設定に初期化されます。

□ データベース初期化

データベース内のユーザーデータをすべて削除します。ユーザーの静脈データ、制御情報、およびタイムゾーン表が削除されます。

□ イベント初期化

ユーザーの履歴とシステムログがすべて削除されます。

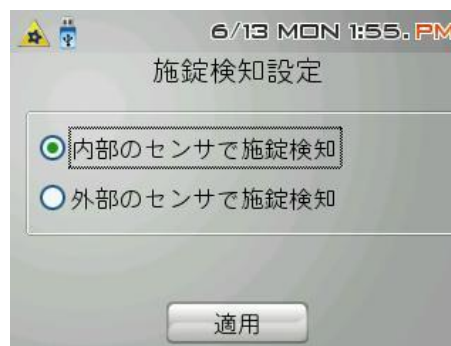


2.7 施錠検知設定

VP-II XG をドアコントローラとして使用する場合、ドアロックがドアの施錠および解錠に使用されます。この場合、ドアロックシステムはドアを制御するためのセンサを内蔵していますが、場合によっては、ドアロックにこのセンサがないことがあります。

センサがない場合、VP-II XG からドアの解錠または施錠のための信号をドアロックに送ることができます。このためには、[外部のセンサで施錠検知]オプションを選択します。

管理者メニュー > 3. システム設定 > 8. 施錠検知設定 【デフォルト値: 内部のセンサで施錠検知】

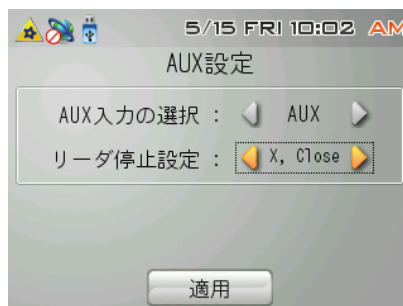


2.8 AUX 設定

管理者メニュー > 3. システム設定 > 9. AUX 設定

【デフォルト値: AUX 入力の選択: AUX、リーダ停止設定 Disable】

Wiegand 入力ポートを 2 個使用できるようにするには、VP-II X の AUX ポートが Wiegand 入力も受け付けるように設定します。これにより、2 つめの Wiegand カードリーダを外部リーダとして使用できます。VP-II の AUX ポートを Wiegand 入力として設定した場合、VP-II X はバイパスモードで稼動し、1) 使用者の有効期限、2) 使用者の有効化、3) ゲートのタイムゾーンの使用者認証オプションだけをチェックします。Wiegand と AUX の違いの詳細については、「第 4 章 2.2 ポートと接続」を参照してください。リーダ停止設定は AUX 入力ポートの IN0-GND 間に設定された無電圧接点信号 (Close/Open) が入力された時に、VP-II X の LCD 画面に「リーダ停止中」と表示され、信号入力が解除されるまで VP-II X の全て操作が無効となります。また VP-II XG 使用時には XG の AUX ポートを使用することもできます。



リーダ停止設定

: **Disable (デフォルト値)**

: X, Close (AUX: IN0-GND間 N.O.)

: X, Open (AUX: IN0-GND間 N.C.)

: XG, Close (AUX: IN0-GND間 N.O.)

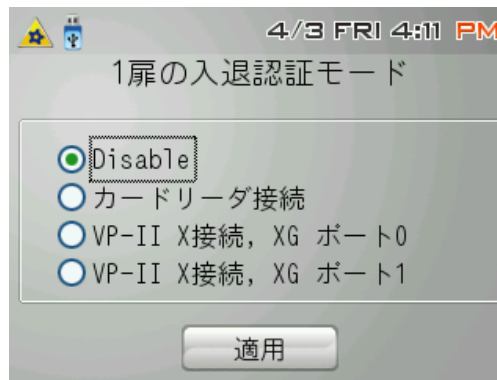
: XG, Open (AUX: IN0-GND間 N.C.)

2.9 1 扉の入退認証モード

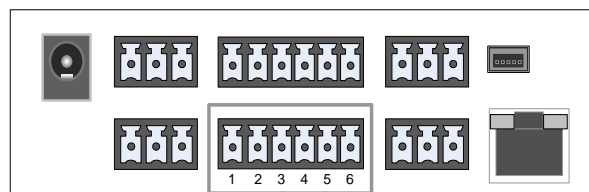
管理者メニュー > 3. システム設定 > 10. 1 扉の入退認証モード【デフォルト値: Disable】

VP-II XG をドアコントローラとして使用し、VP-II XG 1 台に対し、VP-II X を 2 台接続して入室、退室を管理する場合、または前項 2.8 AUX で設定で AUX ポートを Wiegand ポートとして設定した場合に Wiegand カードリーダーを接続することにより、簡易的な入室管理が可能になります。

- カードリーダー接続：入室側で接続する VP-II X に Wiegand カードリーダーを接続
- VP-II X 接続, XG ポート 0：入室側で接続する VP-II X
- VP-II X 接続, XG ポート 0：退室側で接続する VP-II X



Wiegand 入出力ポート



Wiegand入力／出力	
1	入力D0
2	入力D1
3	GND
4	出力D0
5	出力D1
6	GND

3. 運用設定

3.1 モード設定(ネットワーク/シリアル)

管理者メニュー > 2. 運用設定 > 1. モード設定 【デフォルト値:ネットワークモード】

現在サポートされているのはネットワークモードだけです。シリアルモードは将来用であり、現在は使用できません。デフォルトの設定をそのまま使用してください。

3.2 テストモードの解除

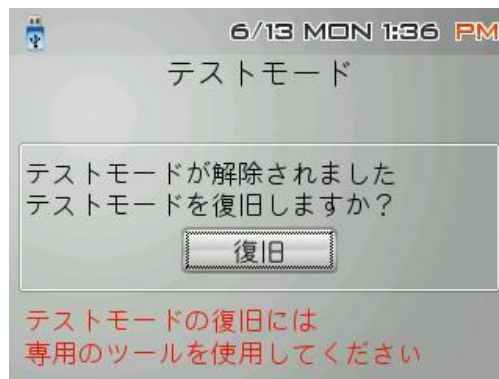
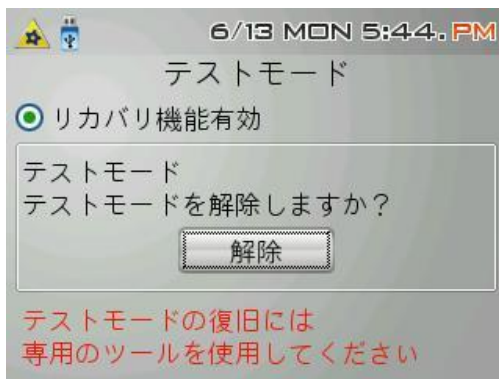
導入が完了し、管理者がシステムの使い方を習得して、何の問題もなく管理者として認証できるようになったら、テストモードの解除をお勧めします。テストモードの概要と機能の詳細については、「1.3 テストモード」を参照してください。テストモードを解除するには、下のメニューを使用します。

管理者メニュー > 2. 運用設定 > 2. テストモード 【デフォルト値:リカバリ機能有効】

テストモードを解除した場合、インストーラを登録するためのテストモードメニューが表示されなくなります。テストモードを解除する方法には2通りあります。

テストモードを解除する前に[リカバリ機能有効]を選択すると、このメニューでテストモードに戻すことができます。[リカバリ機能有効]を選択してテストモードを解除した後で、このメニューに再アクセスすると、[テストモードを復旧しますか?]というメッセージが表示され、テストモードを再度有効にできます。

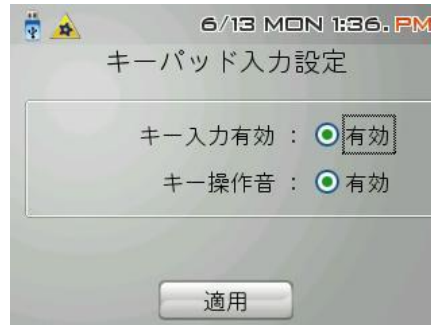
[リカバリ機能有効]を選択せずにテストモードを解除した場合、テストモードに戻すには、機器を工場または販売店に返送する必要があります。これはセキュリティを高めるための機能なので、テストモードをリカバリするには、製造元に返送する必要があります。



3.3 キーパッド入力設定

必要に応じて、キーパッド入力を無効にすることができます。無効にした場合、すべてのキーが応答しません。元に戻すには、管理者がカードで認証してこのメニューにアクセスするか、NetControl-X ソフトウェアを使用して、キーパッドを再度有効にする必要があります。キー入力のサウンドを無効にして、無音で運用することもできます。

管理者メニュー > 2. 運用設定 > 3. キーパッド入力設定 【デフォルト値: 全て有効】



3.4 スリープモード

このオプションが有効(工場出荷時のデフォルト値 - 待機時間(分):1(1~10)、検知距離:7(50cm))である場合、設定された時間内で使用者がいなければ、VP-II X はスリープモードに入ります。これは、電力消費を最小限に抑えるだけでなく、システムの寿命を最大限延ばすためでもあります。スリープモードでは、キーパッドのLED やディスプレイのバックライトは最低限になりますが、VP-II X の IR センサが使用者を検知すると、通常の動作に戻ります。

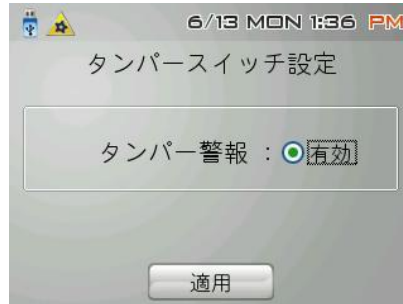
管理者メニュー > 2. 運用設定 > 4. スリープモード 【デフォルト値:7】



3.5 タンパースイッチ設定

タンパースイッチは背面カバーに装備されています。VP-II X を不正に壁のバックプレートから外すと、VP-II X によりこのスイッチが作動します。この設定が有効な場合、VP-II X は、タンパースイッチを検知すると警報を鳴らし、サーバにイベントを送信します。保守のために壁から VP-II X を外す場合は、この機能を無効にすることをお勧めします。

管理者メニュー > 2. 運用設定 > 5. タンパースイッチ設定 【デフォルト値: 有効】



3.6 DB 検索オプション

データベースの検索順序(ローカル、ネットワーク、または両方)を設定できます。デフォルトでは、最初にローカルデータベースのユーザーデータを検索し、何らかの理由でローカルデータベースからデータを取得できなかった場合は、ネットワーク(マスタのデータベース)から検索します。これを、ネットワーク環境の必要に応じて変更できます。この機能はスレーブユニットでのみ使用できます。マスタユニットは常に、自身のデータベースを参照します。

管理者メニュー > 2. 運用設定 > 6. DB 検索オプション 【デフォルト値: 1st: Local, 2nd: Network】



スレーブユニットでの表示画面

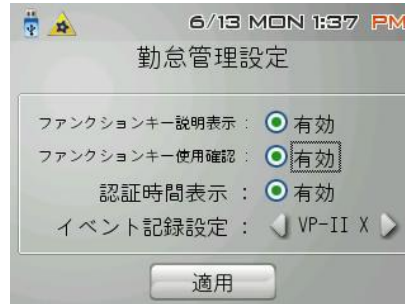


マスタユニットでの表示画面

3.7 勤怠管理設定

勤怠管理に適した画面表示に設定することができます。ファンクションキーの説明表示を「出勤」、「退勤」、「外出」、「戻り」と表示できるファンクション説明表示、ファンクションキーの押し忘れを防止するファンクション使用確認、認証時間の表示などの設定が行えます。

管理者メニュー > 2. 運用設定 > 7. 勤怠管理設定 【デフォルト値: 全て無効】



4. UI 設定

4.1 言語設定

VP-II X では、複数の言語がサポートされています。

管理者メニュー > 4. UI 設定 > 1. 言語設定 【デフォルト値: 日本語】

4.2 サウンド設定

管理者メニュー > 4. UI 設定 > 2. サウンド設定 【デフォルト値: 音量: 3、キー操作音: Sound7、音声: 無効】

□ ボリューム

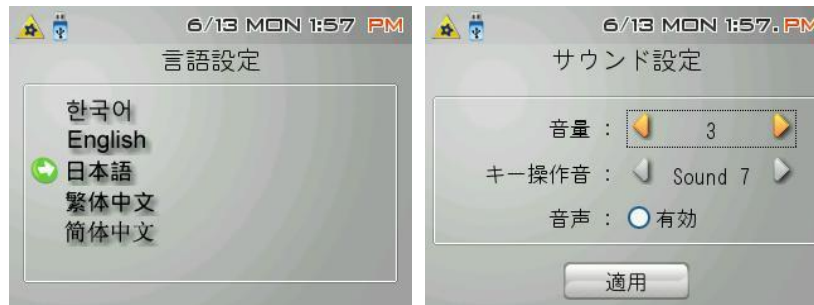
スピーカーのボリュームを 0(無音)から 10(最大)に設定できます。

□ キーパッドサウンド

キー入力のサウンドを 7 種類の音から選択できます。

□ 音声

一部の操作では、「認証に成功しました」など音声によるメッセージがサポートされています。



4.3 PIN 表示オプション

工場出荷時のデフォルトでは、使用者が入力している PIN は表示されません。

管理者メニュー > 4. UI 設定 > 3. PIN 表示オプション 【デフォルト値:無効】



4.4 時計表示

2 タイプの時計および時計表示(12 時間/24 時間)を選択することができます。

管理者メニュー > 4. UI 設定 > 4. 時計表示 【デフォルト値:時計選択:Type 1、時計システム:12-hour】



5. IC Card 設定

5.1 Wiegand 設定

5.1.1 Wiegand 出力

使用者の認証に成功すると、外部他入退室管理システムを持つインターフェースへの Wiegand コードが出力されます。

(1)カード使用者(HID Prox カードまたは IC カード)の場合は、カードから読み取られた Wiegand コードが出力されます。

(2)PIN 使用者の場合は、あらかじめ設定された形式に従って作成された Wiegand コードが出力されます。そのため、PIN 使用者向けに Wiegand 形式を設定する必要があります。また、[ID 認証]に対するサイトコードの値を設定する必要もあります。詳細については、「5.1.3 Wiegand 出力オプション」を参照してください。

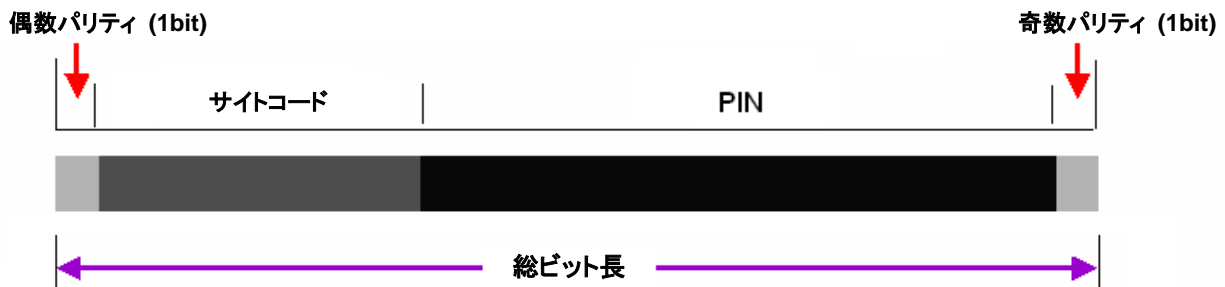
VP-II X は、認証失敗や脅迫警報コードを伴う非常事態についても Wiegand コードを出力できます。

5.1.2 Wiegand 形式の設定

管理者メニュー > 5. IC カード設定 > 1. Wiegand 設定

□ ビット長

トータルのビット長(26~128)とサイトコードのビット長(0~32)の両方を設定します。PIN のビット長は自動的に設定されます。PIN 使用者に対して VP-II X により生成される Wiegand 形式は次のとおりです。



$\text{PIN (またはカード番号) のビット長} = \text{総ビット長} - \text{サイトコードのビット長} - 2 (\text{偶数/奇数パリティビット})$

たとえば、Wiegand コードが 26 ビットでサイトコードが 8 ビットの場合、PIN のビット長は 16 ($26 - 8 - 2 = 16$) になります。

□ HID 1000Card

VP-II X で HID Corporate 1000 Card をサポートするには、次のように[HID 1000Card]オプションを選択する必要があります。



HID Corporate 1000 Card の形式は、標準 Wiegand 形式と同じではありません。このカード形式を適切に設定する方法については、カードの販売元または設置担当者にお問い合わせください。

□ パリティビット

偶数パリティと奇数パリティはそれぞれ 1 ビットです。偶数パリティはトータルビットの前半分、奇数パリティは残りの半分から計算されます。トータルのビット長が奇数の場合、真ん中のビットは偶数パリティの計算と奇数パリティの計算の両方で使用されます。例：

26 ビットの場合(ビット 0~25)：偶数パリティの計算にはビット 0~12、奇数パリティの計算には 13~25 が使用されます。

37 ビットの場合(ビット 0~36)：偶数パリティの計算にはビット 0~13、奇数パリティの計算には 13~36 が使用されます。ビット 13 は偶数パリティと奇数パリティの両方の計算に使用されています。

5.1.3 Wiegand 出力オプション

VP-II X は、認証の失敗または緊急事態通知(脅迫警報コード)についても Wiegand コードを出力できます。PACS(他入退室管理システム)にこれらのコードの違いを認識させるには、それぞれに異なるサイトコードを割り当てる必要があります。

出力有効	サイトコードの値	説明
認証成功	0 ~ 65535	PIN 使用者の認証成功時に使用されるサイトコード。使用者が PIN で認証したときに Wiegand コードを出力するには、このオプションを有効にしてサイトコードの値を指定する必要があります。 カード使用者の場合、カードから読み取られた Wiegand コードが PACS に直接渡されるため、ここで設定されたサイトコードは影響しません。

認証失敗	0 ~ 65535	認証が失敗したときに使用されるサイトコードを設定します。 このオプションが有効化されている場合、PIN 使用者とカード使用者の両方について、元の Wiegand コードのサイトコードがこの値で置き換えられます。 受信側機器 (PACS) も、異なるサイトコードを認識できるように適切に設定しておく必要があります。
脅迫警報	0 ~ 65535	使用者が脅迫認証を実行して非常事態を通知する場合 (脅迫認証の詳細については「4.6 脅迫警報コードを使った認証」を参照)、このサイトコード値が、前述の認証失敗のケースと同じように使用されます。

5.2 MIFARE/iClass カード

IC カード (MIFARE または HID iClass) を使用するには、カードのタイプに適したリーダモジュールを VP-II X の内部に設置する必要があります。

IC カードの使用者については、静脈データや個人情報を含む使用者データはカードに保存されますが、必要であれば、システムメモリに保存することもできます。

□ サポートされているカードのタイプ

MIFARE	1K、4K、DESFire
HID iClass	16K/16、16K/2、32K(16K/2+16K/1)、32K(16K/16+16K/1)

次のメニューを使用して、カードのアクセスに必要なパラメータを適切に設定します。

管理者メニュー > 5. カード設定 > 2. MIFARE カード
 管理者メニュー > 5. カード設定 > 3. HID iClass カード



□ Reader Status

リーダモジュールのステータスを示します。上の例では、リーダモジュールが設置されていないため、「Not Installed」と表示されています。

□ Start Sector/Start Page

VP-II X のテンプレートで使用されるセクター(MIFARE)またはページ(HID iClass)を設定します。使用者 1 人のデータを保存するために必要なスペースは、Mifare で 7 セクター、HID iClass で 2 ページです。

□ Blank Card Type(MIFARE)

MIFARE カードには 2 種類ありますが、VP-II X では、カードへのアクセスに使用されるキーに基づいて、カードの種類が自動検知されます。カードのタイプは、ブランクの値をチェックすることで認識されます。ブランクの値は FF か AB のどちらかです。どちらかわからない場合は、[チェック]機能を使って情報を取得してください。[チェック]機能は、リーダモジュールが設置されている場合のみ使用できます。

□ Cache Mode(HID)

Cache モードが有効な場合、VP-II X は、あとでより速い読み取り操作ができるように、カードから読み込んだ使用者データを内蔵メモリにキャッシュします。

□ DB dependence

IC カード使用者を登録した場合、カードの UID(ユーザ識別子)番号が管理のために VP-II X データベースに保存されます。登録した使用者の UID 番号は、ネットワーク上の VP-II X ユニットすべてに複製されます。

このオプションを選択した場合、IC カードに別の VP-II X システムが発行した静脈データが入っていたとしても、VP-II X のデータベースにそのカードの UID 番号が登録されていない場合は、カードは受け付けられません。

選択されていない場合、VP-II X は、データベースで UID をチェックせずにカードを受け付けます。

□ カスタマーキーの設定

VP-II X は、IC カードに保存されているデータの暗号化にキーを使用します。セキュリティ上の理由により、1 つのキーをすべての VP-II X 機器で使用してください。このキーは VP-II X とカードの両方に保存され、カードに保存されたキーが VP-II X のキーと一致しなければ、カードは受け付けられません。これにより、別のサイトで発行されたカードなど権限のないカードがサイトで認証されないようにすることができます。

□ UID Order(MIFARE)

VP-II X は、MIFARE カードの UID を使用して、そのカードの Wiegand データを生成します。これには、MSB(最上位ビット)と LSB(最下位ビット)の 2 つのタイプがあります。VP-II X はデフォルトで MSB に設定されています。下の例は、MSB が選択されているときに Wiegand データがどのように生成されるかを示しています。

下の表は、VP-II X が、各種 MIFARE カードを使用して Wiegand データを送信する方法と、MSB オプションを使用して Wiegand データを生成する方法を示しています。

MIFARE カード	UID	最大ビット(パリティビットを含む)
1K/4K	4 バイト(32 ビット)	34 ビット
DESFire	7 バイト(56 ビット)	58 ビット

UID 16 進数値:[12H][34H][56H][78H]

偶数パリティ	12H	34H	56H	78H	奇数パリティ
1	0001 0010	0011 0100	0101 0110	0111 1000	1

UID を登録した後で、管理者が UID の順番を変更する場合、正しい Wiegand データ形式を取得するには、すでに登録したカードを再登録する必要があります。

5.3 ASI4000 設定

管理者メニュー > 6. IC カード設定 > 4. ASI4000 設定【デフォルト値:MSB】

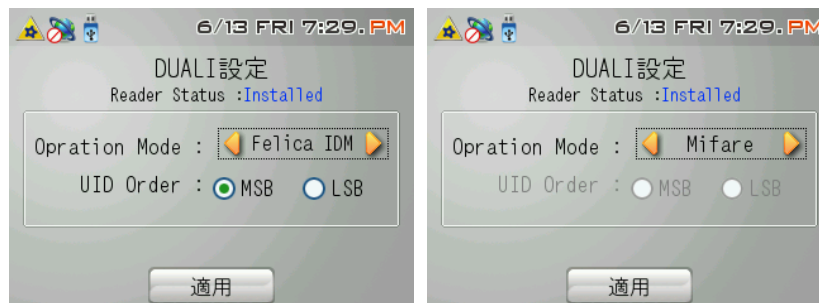
FeliCa IDm モジュール使用時に MSB/LSB のいずれかを設定することができます。



5.4 DUALI 設定

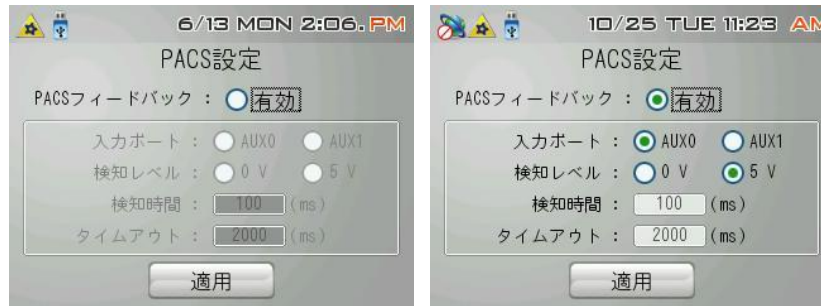
管理者メニュー > 6. IC カード設定 > 5. DUALI 設定【デフォルト値: Operation Mode: FeliCa IDm】

NFC モジュール使用時に FeliCa IDm または MIFARE を設定することができます。また FeliCa IDm 設定時には MSB/LSB のいずれかを設定することができます。



5.5 PACS(Physical Access Control Security)設定

PACS(他入退室管理システム)と VP-II X の間の信号コミュニケーションを確認するには、PACS フィードバックを有効にします。



□ 入力ポート

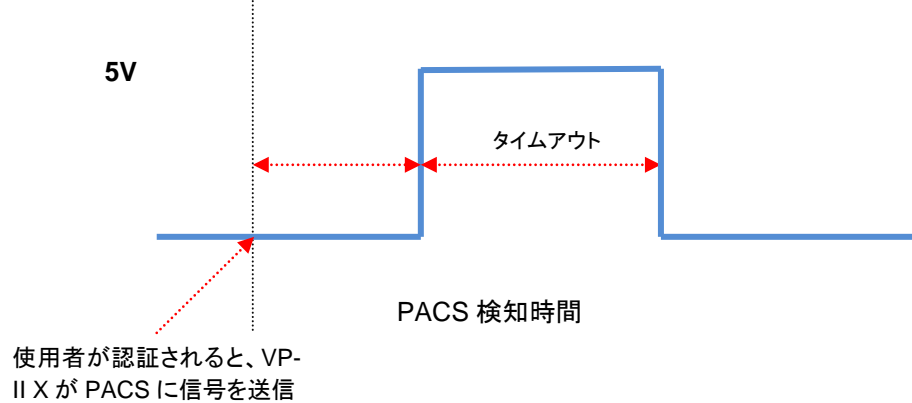
ここでは、信号が使用する入力ポートを選択します。2つのAUXポートが利用できます。AUXポートの詳細については、「2.2 ポートと接続」を参照してください。

□ 検知レベル／検知時間

検知レベル信号はPACSからVP-II Xに送信されます。検知時間は、PACSがVP-II Xに応答するまでの予想時間です。VP-II Xが0Vか5Vのどちらの信号を検知するかを設定できます。

□ タイムアウト

タイムアウトには、VP-II XがPACSからの信号を待機する時間を設定します。設定できる最小値は50ミリ秒です。タイムアウト時間内にVP-II Xが信号を受信しなかった場合、VP-II Xにメッセージ(「アクセス承認」または「アクセス拒否」)が表示されます。



6. ツール

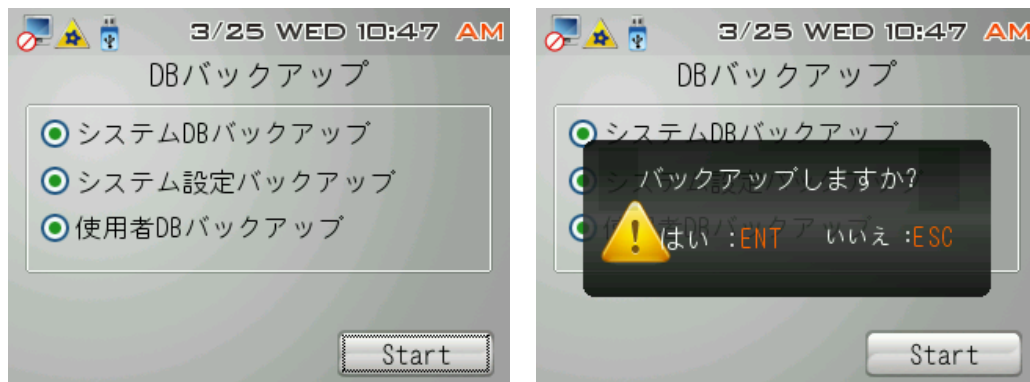
6.1 DB バックアップ／リストア

この機能は、VP-II X のシステム DB、システム設定、使用者 DB を USB メモリにバックアップできる機能です。また VP-II X の故障時、バックアップをしてあれば、交換機器にバックアップデータをリストアすることができ、復旧が容易となります。

6.1.1 DB バックアップ

USB メモリを挿入後、バックアップしたい項目にチェックを入れます。

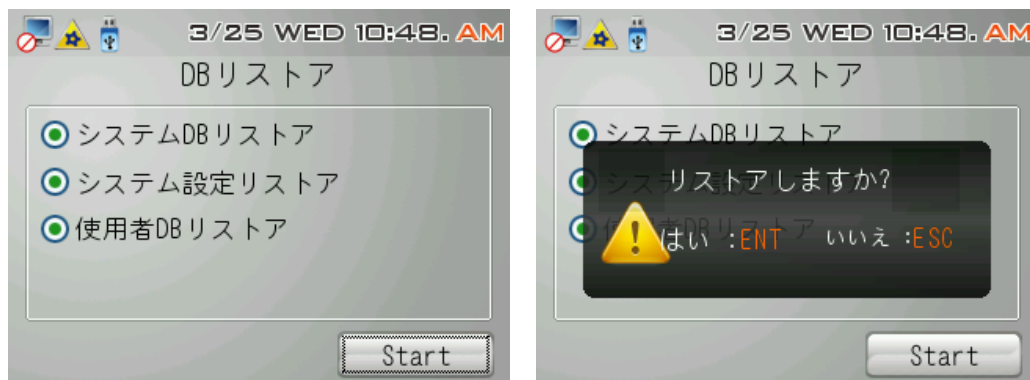
管理者メニュー > 6. ツール > 1. DB バックアップ／リストア > 1. DB バックアップ



6.1.2 DB リストア

USB メモリを挿入後、バックアップしたい項目にチェックを入れます。リストア成功後、VP-II X は自動的に再起動します。

管理者メニュー > 6. ツール > 1. DB バックアップ／リストア > 2. DB リストア



6.1.3 イベントログのバックアップ

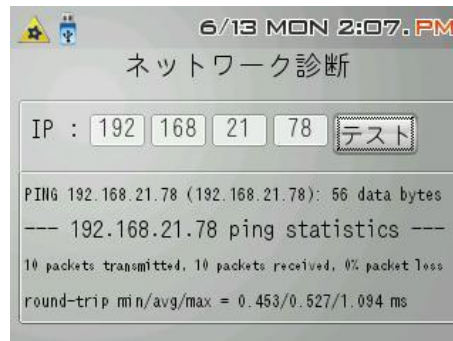
この機能の使い方については、7. イベントレポートビューワを参照してください。

6.2 診断ツール

6.2.1 ネットワーク診断

この機能は、現在のネットワークステータスのテストと、IP ネットワーク経由でホストにアクセスできるかどうかを判断するために使用します。管理者が[テスト]メニューを選択すると、VP-II X は IP アドレスで指定された機器にテストパケットを送信します。約 10 秒後、VP-II X に結果が表示されます。このツールを使用して、ネットワーク設定に問題があるかどうかを判断できます。

管理者メニュー > 6. ツール > 2. 診断ツール > 1. ネットワーク診断



6.2.2 ネットワーク情報

これは、現在のネットワーク設定 (IP アドレス、サブネットマスク、ゲートウェイ、サーバ IP、マスタ IP、ポート) を表示します。この情報を見て、VP-II X のネットワーク設定を確認できます。

管理者メニュー > 6. ツール > 2. 診断ツール > 2. ネットワーク情報



6.3 ソフトリセット

この機能により、背面の電源コードを抜かずに、必要なときにVP-II Xを再起動することができます。

管理者メニュー > 6. ツール > 3. ソフトリセット



□ Socket Restart

VP-II X は、スキャナと関連しているネットワークプロトコルをすべてリセットし、再起動します。

□ Soft Reset

管理者がシステムを再起動したい場合、この機能を使用できます。

第 4 章 付録

第4章 付録

1. ファームウェアのアップグレード

VP-II X に適用されるファームウェアファイルは 5 種類あります。これらのファイルのアップグレードが入手可能になった場合、簡単にアップグレードできます。ファームウェアファイルには、Boot、Kernel、Ramdisk、Application、Media があります。下の例に示すとおり、ファームウェアファイルの拡張子は「vpx」です。

kernel-0.1.2.v1.vpx

app-0.1.12.v60.vpx

ファームウェアは USB メモリ機器かネットワーク上の XConfig アプリケーションソフトウェアを使用して、VP-II X にダウンロードできます。

□ USB メモリによる

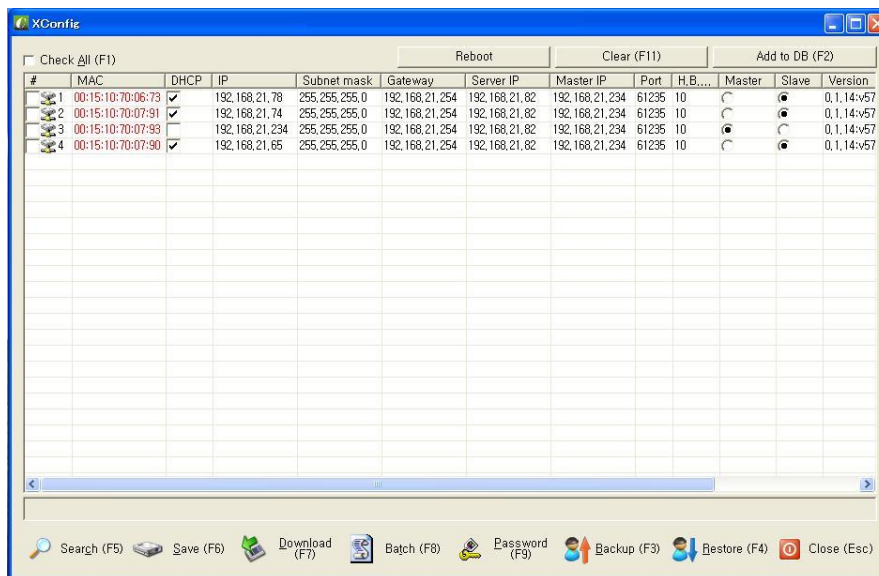
USB メモリを使用してファームウェアをダウンロードする方法については、「2.2 ファームウェア情報」を参照してください。

□ アプリケーションソフトウェア(XConfig)による

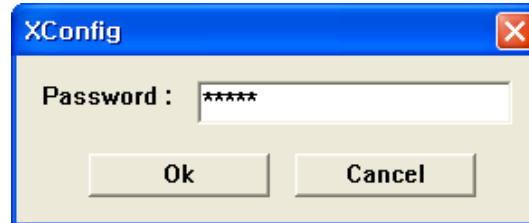
ファームウェアファイルを、VP-II XConfig ソフトウェアのダウンロード機能を使用して、VP-II X にダウンロードできます。物理的に VP-II X ユニットのところへ行く必要がなく、同時に複数の VP-II X ユニットのファームウェアをアップグレードする場合に便利です。

XConfig ソフトウェアは NetControl-X アプリケーションソフトウェアパッケージに含まれます。また、必要に応じて別途入手することもできます。XConfig のインストール方法と使用方法の詳細については、NetControl-X の取扱説明書を参照してください。

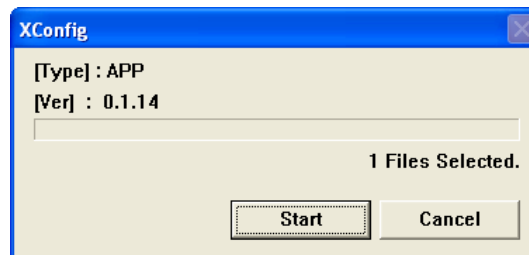
[Search]ボタン(F5)をクリックすると、ネットワークで使用できる VP-II X がすべて表示されます。ファームウェアをダウンロードする VP-II X を 1 台以上選択します。次の例では、2 台の VP-II X が選択されています。



ファームウェアファイルをロードするには、[Download] (F7) をクリックし、次のウィンドウが表示されたら、パスワードを入力します。デフォルトのパスワードは「admin」です。



Windows のファイル検索ウィンドウからファームウェアファイルを選択し、[Start] ボタンをクリックして、ダウンロードを開始します。



完了メッセージが表示されるまで待ちます。また、VP-II X にもダウンロードの進捗状況が表示されます。VP-II X は、フラッシュメモリにファームウェアを書き込むと、自動的に再起動します。メモリに完全にファームウェアを書き込むには、VP-II X の電源を入れたままにしておく必要があります。ファームウェアのアップグレード中に電源を切ると、ファームウェアのインストールが不完全になり、システムが動かなくなる可能性があります。

2. 簡易設置説明書

2.1 VP-II X の設置場所

□ 設置環境

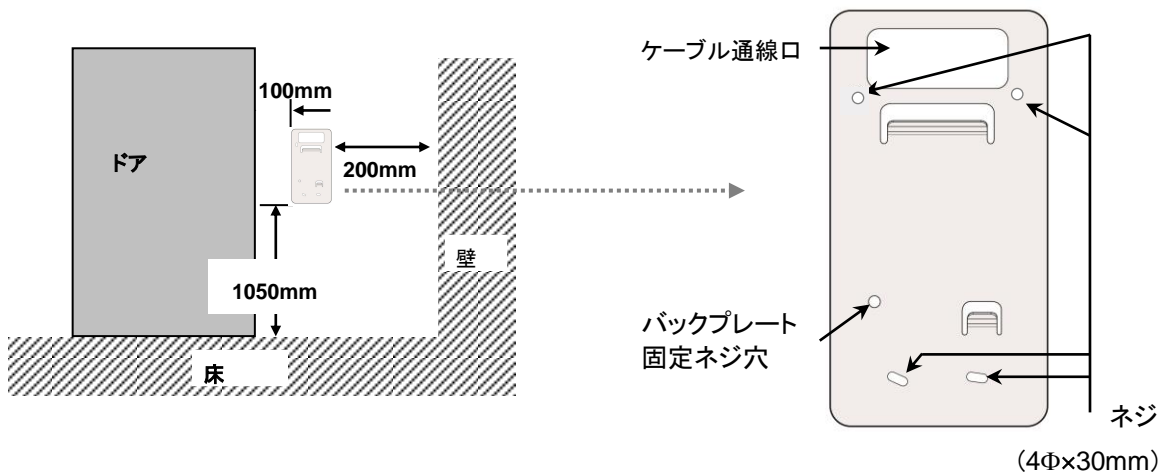
VP-II X は 20,000 lux を超える直射日光が当たらない屋内に設置してください。

傾斜している場所には絶対に VP-II X を設置しないでください。傾斜している場所に設置すると、手を入力したときの使用者の姿勢が不安定になり、システムのパフォーマンスが低下する可能性があります。

□ バックプレートの設置

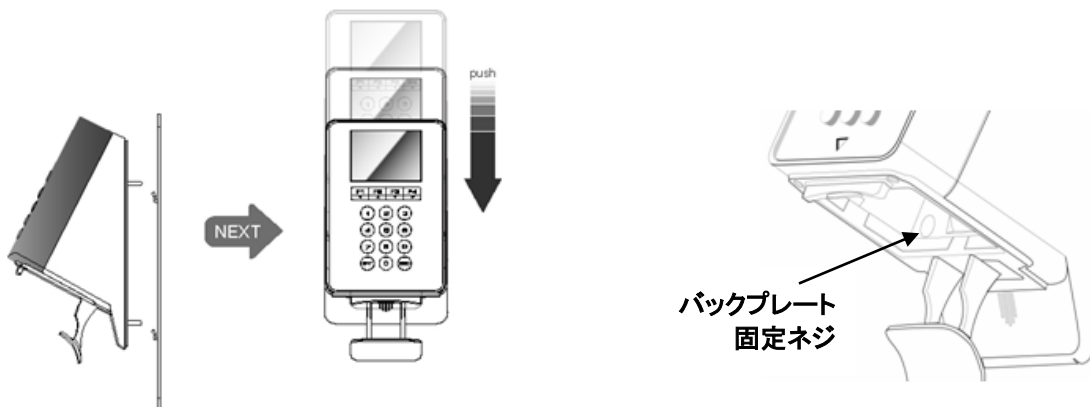
VP-II X は床からの高さが 1,050mm で、ドアの枠から 100mm のところに設置します。右側に外壁がある場合、使用者がきちんと立って、手を入力できるように、VP-II X は、その壁から少なくとも 200mm 離れたところに設置してください。

VP-II X を設置するためのバックプレートを設置場所に置き、ケーブル通線口の位置を確認してから、穴を開けます。バックプレート用ネジを使って、バックプレートを壁に固定します。

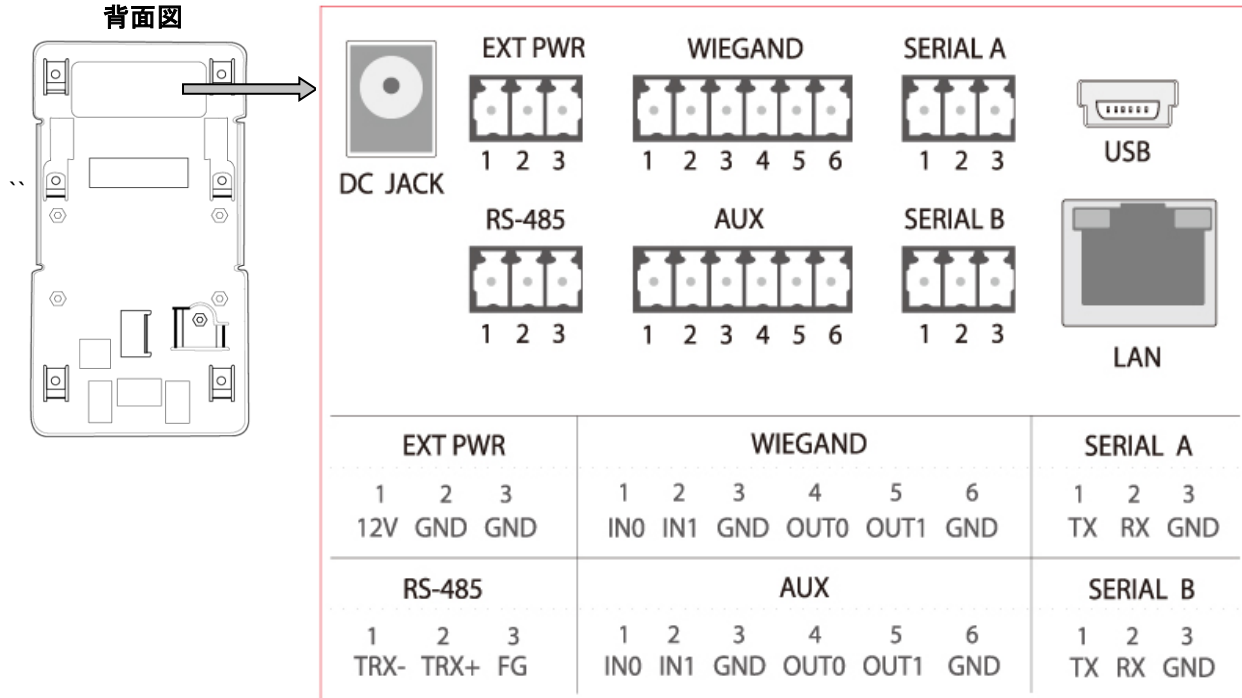


□ VP-II X の設置

バックプレートに VP-II X を当てがい、下まで押し込みます。センサモジュールの筐体にあるバックプレート固定ネジを使用して、バックプレートに VP-II X を固定します。



2.2 ポートと接続



□ 電源入力

VP-II X への電源供給は VP-II XG または AC アダプタから供給されます。必要な電源は DC 12V~15V、0.5A です。

□ USB ポート

この USB ポートは、生産時のテストと工場出荷時の初期設定の目的でのみ使用されます。お客様が使用するものではありません。

□ LAN

ネットワークに接続する場合は、RJ45 コネクタ付きイーサネットケーブルを接続します。

□ Wiegand

これらはカードリーダーからの入力、または他入退室管理システム (PACS) への出力、もしくはその両方に使用される Wiegand インターフェースポートです。IN0 は入力用 Wiegand D0 信号、OUT0 は出力用 Wiegand D0 信号を表します。

VP-II X は標準 Wiegand インターフェース信号を生成します。Wiegand 機器の最大接続距離は、完全にシールドされているか、または 5 本のツイストペアで構成されている 22AWG ケーブル使用時に 150m です。ケーブルの仕様によっては、通信可能距離が短くなる可能性があります。

□ AUX

AUX ポートは、外部システムと連動するための TTL レベル(+5V) デジタル入力／出力ポートです。2 個の入出力ポートが用意されています。これらのポートは、大型 LED やランプなどの外部インジケータに対する PACS からのアクセス許可信号入力、火災警報入力、認証失敗／成功出力に使用されます。ただし、これらの機能は標準製品には含まれていません。要求に応じて、カスタマイズされたファームウェアの形で提供されます。

□ シリアル A/B

シリアルポート A は、VP-II XG ドアコントローラの接続に使用します。接続は次の表のとおりです。

VP-II X Serial Port A			VP-II XG RS232 Port	
1	Tx	↔	3	Rx
2	Rx	↔	2	Tx
3	GND	↔	1	GND

シリアルポート B は将来用のポートのため、現在は使用できません。

□ RS485

VP-II X と VP-II XG の間の距離が 15m を超える場合、RS485 インターフェースを使用できます。ただし、デフォルトでは RS485 モジュールはインストールされていないため、VP-II X と VP-II XG の両方への追加インストールが必要です。RS485 モジュールは別途提供されます。詳細は、製品の販売店にご相談ください。

3. イベントレポートビューア(イベントログのバックアップ)

VP-II X ユニットがサーバを使用しない構成を行うために、Techsphere 社から VP Report というアプリケーションが提供されています。これにより、保存されているイベントを USB メモリにエクスポートして、使用者管理イベントを確認し、診断することができます。

エクスポートされたファイルの名前は「event_bak.db」です。このファイルは VP Report アプリケーションで開くことができます。次の図にレポートの例を示します。このアプリケーションを使用して、[使用者の登録]、[使用者の削除]、[使用者の認証]などの使用者管理イベントを含む、履歴の詳細を表示できます。Techsphere では、すべてのシステムイベントの完全な監査証跡や診断ツールのために、NetControl-X ソフトウェアをインストールしたサーバの使用を強くお勧めします。

管理者メニュー > 6. ツール > 1. DB バックアップ／リストア > 3. イベントログのバックアップ

VP Report

Open Save Language Exit

User Event:

User Enrollment
 Delete User
 User Verification

Search Time: 2010-03-11 10:48 ~ 2010-03-12 10:48

PIN:








	Time	Event Type	Verification User Type	PIN	User Type	Verifi
1	2010-03-12 10:47:35	Verification	User Verification Success	00	Installer	
2	2010-03-12 10:46:52	Verification	User Verification Success	1010	User	
3	2010-03-12 10:46:42	User Enrollment	User Enrollment Success	1010	User	
4	2010-03-12 10:46:23	Verification	User Verification Success	00	Installer	
5	2010-03-12 10:46:17	Verification	User Verification Success	1111	Manager	
6	2010-03-12 10:45:58	Verification	User Verification Success	9999	User	
7	2010-03-12 10:45:52	Verification	User Verification Success	1111	Manager	
8	2010-03-12 10:45:43	Verification	User Verification Success	8888	User	
9	2010-03-12 10:45:25	Verification	User Verification Success	1111	Manager	
10	2010-03-12 10:45:19	Verification	User Verification Success	9999	User	
11	2010-03-12 10:45:13	Verification	User Verification Success	8888	User	
12	2010-03-12 10:44:59	User Deletion	Delete User Success	17	User	
13	2010-03-12 10:44:25	User Enrollment	User Enrollment Success	9999	User	
14	2010-03-12 10:43:59	User Enrollment	User Enrollment Success	8888	User	
15	2010-03-12 10:43:42	Verification	User Verification Success	00	Installer	
16	2010-03-12 10:43:09	Verification	User Verification Failure - Not allowed verification	5555	User	

Total Count : 21

File Path = [C:\desktop\Manuals\report\event_bak.db]

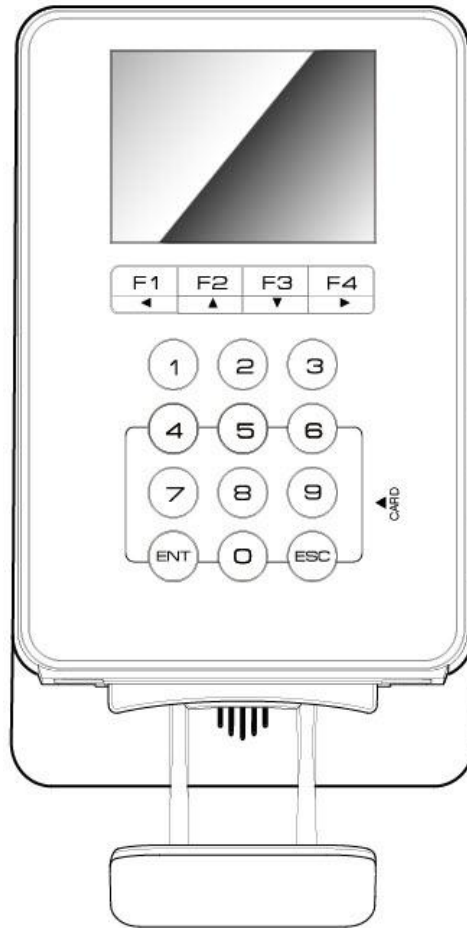
4. トレイアイコン

現在の VP-II X のステータスがアイコンで表されます。アイコンを見れば、VP-II X の現在のステータスがすぐにわかります。アイコンとその説明については、下の表を参照してください。

アイコン	ステータス	ヒントとトラブルシューティング
	ネットワークに接続されていません	<ol style="list-style-type: none"> 1. ネットワークケーブルの接続を確認してください。 2. 現在のシステムでのネットワーク設定を確認してください。 ⇒ IP アドレス、ゲートウェイ、サブネットなど。 3. ping コマンドを使って、ネットワークステータスを確認してください。 4. ネットワーク管理者に問い合わせてください。
	サーバに接続されていません	<ol style="list-style-type: none"> 1. サーバ設定を確認してください。 2. サーバのステータスを確認してください。 3. ネットワーク管理者に問い合わせてください。
	マスタに接続されていません	<ol style="list-style-type: none"> 1. 管理者メニューでマスタ機器の設定を確認します。 2. マスタ機器のステータスを確認します。 3. ネットワーク管理者に問い合わせてください。
	タンパースイッチからの警告です	<ol style="list-style-type: none"> 1. VP-II X のステータスを確認してください。 2. VP-II X の設置状態およびタンパースイッチ設定を確認してください。 3. タンパースイッチが機能していることを確認してください。
	テストモード	<ol style="list-style-type: none"> 1. VP-II X はテストモードで動作しています。テストモードを解除すると、このアイコンが表示されなくなります。
	VP-II XG が接続されていません	<ol style="list-style-type: none"> 1. VP-II XG と VP-II X の間の接続を確認してください。 2. VP-II XG のステータスを確認してください。 3. VP-II XG の設定を確認してください。
	USB メモリが接続されています	<ol style="list-style-type: none"> 1. USB メモリが接続されています。

NetControl-X

Application software for VP-II X
Hand Vascular Pattern Recognition (HVPR) System



取扱説明書

Ver.1.3



Hand Vascular Pattern Recognition

はじめに

手の甲静脈認証(HVPR)システム VP-II X をお買い上げいただき、まことにありがとうございます。

この説明書では、手の甲静脈認証システム VP-II X による入退室管理および勤怠管理に使用されるアプリケーションソフトウェア NetControl-X の機能や特徴を説明します。

VP-II X は生体認証スキャナで、赤外線ベースのセンサ機器を使用して、手の甲の表皮の下にある下皮から読み取った、個人個人で異なる静脈パターンを利用して、使用者を認証します。静脈パターンは裸眼では見えず、手の傷や汚れなどには簡単に影響されません。このため、条件の厳しい環境でもパフォーマンスが低下せず、改ざんは 100%不可能で、他の生体認証方式に伴うプライバシーの問題もありません。HVPR テクノロジーの利用により、全人口の 99.98%が認証速度 0.4 秒でシステムを正確に使用することができます。使用者によるボトルネックが解決され、別の通用口を用意する必要がなくなります。VP-II X の詳細については、『VP-II X 取扱説明書』を参照してください。

NetControl-X は、使用者管理、機器管理、機器制御(セキュリティレベル、扉解錠など)、機器モニタリング、イベントモニタリング、ログインアカウント管理、フロアマップ管理、入退室/勤怠レポートなど、入退管理および勤怠管理に必要なさまざまな機能をサポートしています。ユーザーインターフェースは、グラフィック環境を使って開発されており、容易に使用できます。

□ カスタマーサービス

この説明書や弊社製品に関するご質問は、製品販売店に遠慮なくお問い合わせください。プロの技術者がお答えいたします。

株式会社 SYNCHRO

〒102-0073 東京都千代田区九段北 1-10-9 九段 VIGAS 5 階

Tel: 03-4570-3291 FAX: 03-4570-3292

電子メール: message@udc-synchro.co.jp

Web: www.udc-synchro.co.jp

□ 免責事項

本書に記載されている内容は情報提供のみを目的にしています。Techsphere は、不正確または不完全な情報に対して、およびこれらの情報を信頼して行われた行為に対して、一切の責任を負いかねます。

注意:この説明書の内容は、製品の性能向上を反映するために、変更されることがあります。

□ 著作権について

本書は独占所有物です。参照以外の目的では使用しないでください。Techsphere Co., Ltd.は、いかなる時点でも、この製品を変更また製造を停止する権利を保有しています。

目次

はじめに	1
目次.....	2
改訂情報	5
第1章 概要	6
1. 構成.....	6
1.1 ソフトウェアのコンポーネント.....	6
1.1.1 DBMS (MS-SQL)	6
1.1.2 XAgent	6
1.1.3 ソフトウェア保護キー:ワイブキー	6
1.1.4 XConfig	6
1.1.5 NetControl-X	6
1.2 ネットワーク構成	7
1.2.1 マスタ/スレーブ運用	7
1.2.2 ローカルネットワーク構成	7
1.2.3 複数ロケーションのネットワーク接続	8
2. インストールとセットアップ	9
2.1 インストール.....	9
2.2 VP-II Xの構成と登録	9
2.2.1 ネットワークパラメータのセットアップ	9
2.2.2 DBMSへのVP-II Xの登録	9
2.3 XAgentのセットアップ.....	9
2.4 NetControl-Xへのログイン	12
2.5 VP-II XをXAgentに接続.....	12
2.6 パスワード管理	13
2.6.1 ネットワークパスワード.....	13
2.6.2 NetControl-X	13
3. 用語および略語	14
3.1 使用者のタイプ	14
3.2 管理者.....	14
3.3 インストーラ	14
3.4 テストモード	14
3.5 セキュリティレベル	14
3.6 生体識別機能(HCD)レベル	15
3.7 VP-II XG(ドアコントローラ)	15
3.8 アンチパスバック.....	15
3.9 バイパス(PINまたはカードのみの出入:静脈パターン認証なし)	15
3.10 脅迫認証	15
3.11 通知.....	16
第2章 NetControl-Xのメニューと機能	17
1. メニュー.....	17
1.1 メイン画面.....	17
1.1.1 イベントおよび警報表示.....	17

1.1.2	機器モニタリング	17
1.1.3	アイコン	18
1.1.4	機器アイコンメニュー	19
1.1.5	XAgentステータスの確認	19
1.2	メニューの説明	20
2.	プログラム管理機能	22
2.1	ログインアカウント管理	22
2.2	警報機能とメールによる通知	22
2.3	言語および表示オプション	23
2.4	メッセージの変更	24
3.	入退室管理	25
3.1	時間帯／エリア制限による使用者の制御	25
3.2	時間帯制御テーブル	26
3.2.1	祝祭日テーブルの設定	26
3.2.2	時間帯テーブルの設定	27
3.3	アクセスエリアグループ設定	28
3.4	アンチパスバック機能	29
3.5	扉管理機能	31
3.6	Wiegandの設定	32
3.6.1	Wiegandフォーマット設定	32
3.6.2	VP-II X Wiegand出力の設定	34
4.	機器管理	36
4.1	追加／削除 (VP-II X、XAgent、XG)	36
4.2	機器グループ	37
4.2.1	機器のグループ化	37
4.2.2	マップの割り当て	37
4.3	機器設定 (VP-II Xの設定)	39
4.3.1	機器ステータス	40
4.3.2	日付／時間設定	41
4.3.3	サマータイム	41
4.3.4	Wiegand	41
4.3.5	開放時間帯	41
4.3.6	閉鎖時間帯	41
4.3.7	テストモード	41
4.3.8	VP-II Xに表示される通知	41
4.4	データベース同期	43
4.5	VP-II Xから使用者リストとインストーラ情報を取得	43
5.	使用者管理	44
5.1	使用者グループ定義	44
5.2	使用者定義可能なフィールド	44
5.3	使用者の登録	45
5.4	[使用者管理]メニュー	47
5.4.1	認証	47
5.4.2	使用者の削除／管理者の削除	47
5.5	使用者の変更	47
5.5.1	使用者情報／パスワード	48
5.5.2	カスタム定義	48
5.5.3	静脈データ登録／再登録	48
5.6	使用者のインポート／エクスポート／事前登録	49
5.6.1	使用者情報のエクスポート	49
5.6.2	使用者情報のインポート	50

5.6.3 事前登録.....	52
5.7 削除予定の使用者リスト	53
5.8 再登録使用者リスト	53
6. レポート、イベント表示、データベースバックアップ/管理	54
6.1 レポート	54
6.1.1 レポートの共通オプション.....	54
6.1.2 勤怠日報.....	56
6.1.3 勤怠日報 使用者毎	56
6.1.4 入退室レポート.....	57
6.1.5 機器ログ/イベント	58
6.1.6 コマンドログ	58
6.1.7 勤怠日報 (TNA)	58
6.1.8 勤怠日報 使用者毎 (TNA)	58
6.2 イベント表示	58
6.3 データベースバックアップ/整理	59
6.3.1 バックアップ	59
6.3.2 イベント整理	59
6.3.3 コマンド整理	60
第3章 付録.....	61
1. インストール	61
1.1 NetControl-Xをインストールするためのシステム要件	61
1.2 インストール.....	62
1.3 DBMS (MS-SQL) のインストール	63
1.3.1 Microsoft SQL Server 2005 Expressのインストール.....	63
1.3.2 既存のMicrosoft SQL Serverの使用	64
1.3.3 NetControl-Xデータベースのインストール.....	65
1.4 XAgent/ワイブキーのインストール	68
1.5 XConfig/NetControl-Xのインストール.....	68
2. XConfig.....	68
2.1 VP-II Xネットワークパラメータのセットアップ	69
2.2 ファームウェアのダウンロード/アップグレード.....	70
2.3 DBMSへのVP-II Xの登録 — DBへ追加 (F2).....	71
2.4 パスワード/バックアップ/リストア	71

改訂情報

- D0:2009年6月10日 初版
- V1:2009年6月19日 初版発行
- V1.1:2009年6月29日 文法的な訂正
- V1.2:2010年5月25日
 - NetControl-X Version 1.1.45の新規機能を追加
- V1.3:2013年5月30日
 - 11頁 第1章 2.インストールとセットアップ>2.3 XAgentのセットアップ
 - ・DB Backup 補足、説明追記
 - 46頁 第2章 5.使用者管理>5.3 使用者の登録
 - ・登録機 説明追記
 - 58頁 第2章 レポート、イベント表示、データベースバックアップ/管理 6.1 レポート
 - ・6.1.7 勤怠日報(TNA)、6.1.8 勤怠日報 使用者毎 説明追記
 - 61頁 第3章 1.インストール 1.1 NetControl-Xをインストールするためのシステム要件
 - ・各項OSバージョン追記
 - 72~75頁 第3章 2.Xconfig 2.4 パスワード/バックアップ/リストア
 - ・バックアップ/リストア方法の補足、説明追記
 -
 -
 -
 -

第 1 章 概要

1. 構成

1.1 ソフトウェアのコンポーネント

NetControl-X ソフトウェアパッケージは、DBMS、XConfig、XAgent、NetControl-X の 4 つのコンポーネントから構成されています。

1.1.1 DBMS (MS-SQL)

NetControl-X は、データベース管理システム (DBMS) として、Microsoft SQL 2005 Express または互換性のあるバージョンの Microsoft SQL を使用することができます。デフォルトで使用されるのは MS-SQL 2005 Express です。大規模なシステムにおいては、有償版 MS-SQL の使用が推奨されます。既に MS-SQL がインストールされている場合は、新たにインストールするのではなく、既存のものを使用するように NetControl-X を構成することができます。

すべてのコマンドと、コンポーネントや VP-II X ユニット間の通信は、DBMS を通じて行われます。

1.1.2 XAgent

バックグラウンドで実行される XAgent は、VP-II X ユニットとの通信を管理します。XAgent は、DBMS 経由で、NetControl-X から指定された VP-II ユニットにコマンドを転送し、NetControl-X に転送される応答を受信します。また、使用者のトランザクションやシステムログなど、VP-II X で発生するすべてのイベントを収集し、DBMS に格納することにより、NetControl-X や、NetControl-X SDK を使用して実装されるその他のサードパーティアプリケーションで使用できるようにします。

XAgent の設定方法については、「第 1 章 2.3 XAgent のセットアップ」を参照してください。

1.1.3 ソフトウェア保護キー: ワイブキー

NetControl-X を使用するには、XAgent が実行されているサーバの USB ポートにソフトウェア保護ロックキー (ワイブキー) を取り付けておく必要があります。このキーは Techsphere が提供するもので、NetControl-X インストールパッケージに入っています。XAgent は起動時にワイブキーをチェックします。VP-II X が複数ある場合、ワイブキーが見つからないと、XAgent は正しく動作しません。VP-II X ユニットが 1 台の場合、NetControl-X はワイブキーがなくても正常に動作します。

複数のロケーションで複数の XAgent を実行する場合、XAgent を実行するサーバのそれぞれにワイブキーを取り付ける必要があります。

1.1.4 XConfig

XConfig は、VP-II X のネットワークパラメータをセットアップするためのソフトウェアツールです。XConfig はネットワークの TCP/IP ブロードキャスト範囲内から VP-II X ユニットを検索し、IP アドレスやポートなどのネットワークパラメータを設定または変更できます。これはまた、VP-II X にファームウェアをダウンロードする機能を提供します。詳細は「第 3 章 2 XConfig」を参照してください。

1.1.5 NetControl-X

NetControl-X は、アクセス管理や勤怠管理などさまざまな機能を提供する GUI アプリケーションソフトウェアです。この取扱説明書では、NetControl-X 機能の詳細を説明します。

1.2 ネットワーク構成

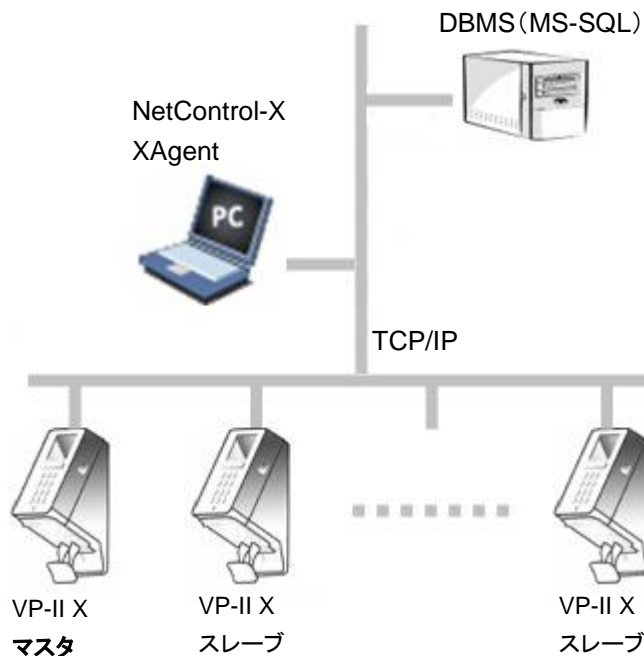
これらのコンポーネントは、1 つのサーバにインストールすることも、複数の異なるサーバ(それぞれのコンポーネントが TCP/IP ネットワークを通じて DBMS サーバに接続できる場合)にインストールすることもできます。コンポーネントを異なる複数のサーバにインストールする場合、ネットワークファイアウォールなど、適切な環境の設定について、ネットワーク管理者に必ず相談してください。

1.2.1 マスタ/スレーブ運用

複数の VP-II X ユニットがネットワークに接続されている場合、そのうちの 1 台をマスタとして設定し、残りをスレーブとして設定する必要があります。XAgent が実行されているサーバをマスタとして設定することもできます。その場合、VP-II X ユニットはすべてスレーブに設定されます。

マスタユニットは、ネットワーク全体に対する使用者のデータベースを管理します。1 つのネットワークにつき、マスタは 1 つのみである必要があります。マスタは、VP-II X でもサーバでも構いません。1 つのネットワークに 64 台を超えるユニットの VP-II X が動作している場合、VP-II X をマスタに設定することはできず、サーバをマスタとして動作させる必要があります。VP-II X がマスタとして設定されている場合、処理できるスレーブは最大 63 ユニットです。

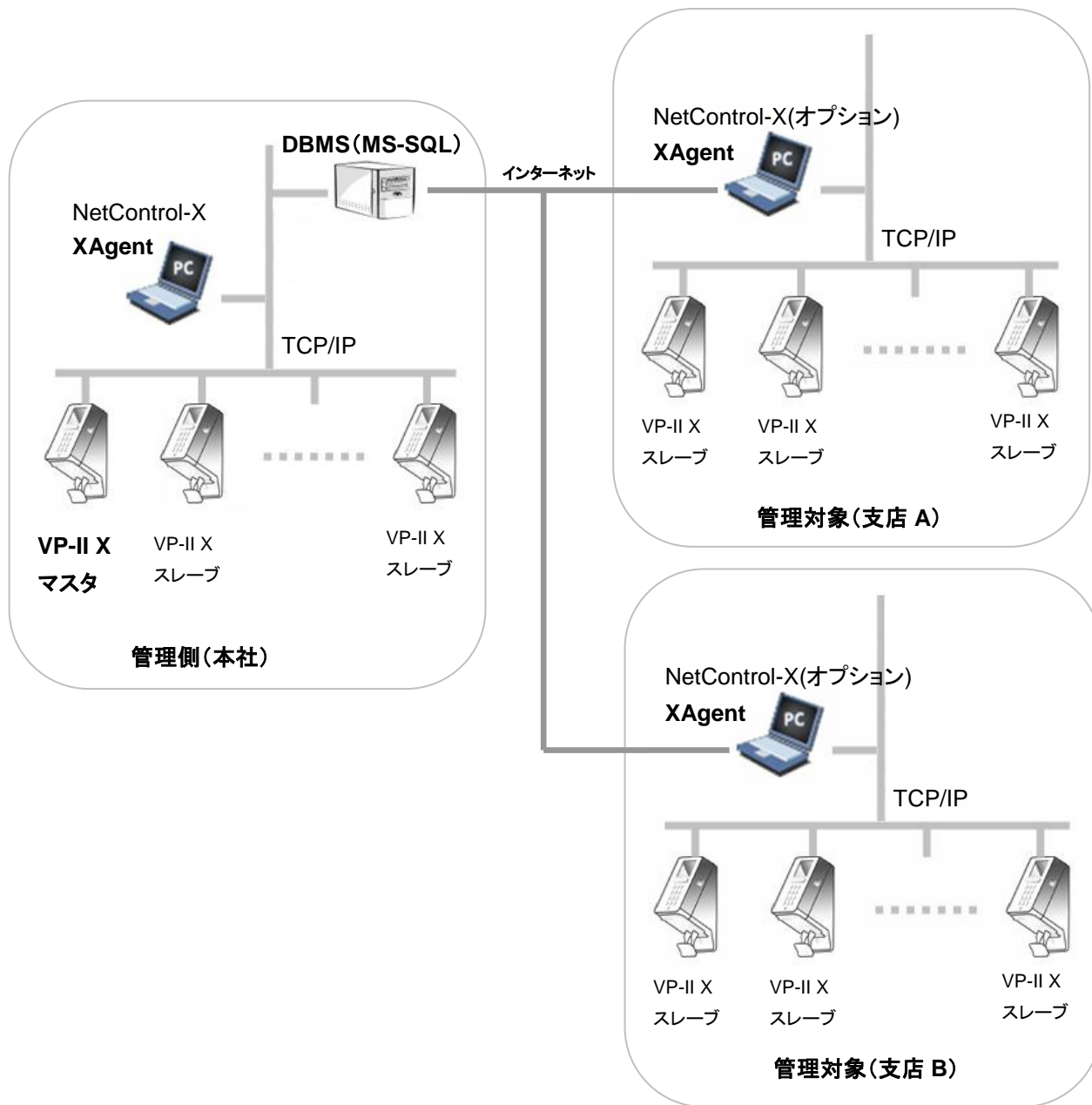
1.2.2 ローカルネットワーク構成



1.2.3 複数ロケーションのネットワーク接続

たとえば、本社、支店 A、支店 B のオフィスなど、さまざまな場所に設置されている複数の VP-II X ユニットの 1 つのシステムとして運用することができます。複数の場所にある VP-II X を適切に動作させるには、1 か所につき XAgent を少なくとも 1 つ実行する必要があります。さらに、これらをお社の DBMS とネットワークで結びます。各支店の VP-II X ユニットの、その場所にインストールされた XAgent により管理されるように割り当てられます。XAgent は、VP-II X ユニットの、DBMS が実行されている中央サーバとネットワークで結びます。また、どの場所でも複数の NetControl-X アプリケーションソフトウェアをインストールできます。ただし、DBMS サーバはシステム全体で 1 つのみである必要があります。

この構成では、あるロケーションで登録したユーザーは、他のすべての場所に、無制限にアクセスできます。



2. インストールとセットアップ

2.1 インストール

NetControl-X ソフトウェアパッケージのインストール方法については、「第 3 章 1 インストール」を参照してください。インストール後、初期設定手順を実行する必要があります。これはシステムを実行するための必須手順です。次の「第 1 章 2.2 VP-II X の構成と登録」から「第 1 章 2.5 VP-II X を XAgent にリンク」までのセクションで説明している手順を実行してください。

2.2 VP-II X の構成と登録

2.2.1 ネットワークパラメータのセットアップ

XConfig ツールまたは各 VP-II X ユニットの管理者メニューを使用して、VP-II X ユニットのネットワークパラメータをセットアップして、これらのユニットが TCP/IP ネットワークを経由して NetControl-X と通信できるようにする必要があります。XConfig を使用したネットワークパラメータのセットアップ方法については「第 3 章 2 XConfig」を参照してください。また、各 VP-II X ユニットで管理者メニューを使用する場合は、『VP-II X 取扱説明書』を参照してください。

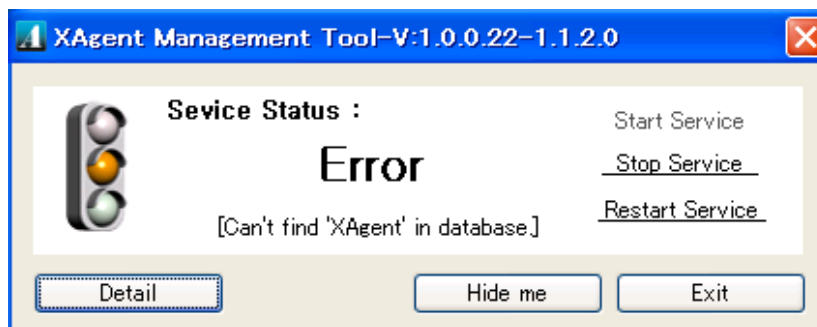
2.2.2 DBMS への VP-II X の登録

VP-II X ユニットの MAC アドレスを NetControl-X データベースに登録する必要があります。選択した VP-II X ユニットのデータベースに自動登録するには、XConfig の[DB へ追加(F2)]機能を使用します。XConfig の使用方法については「第 3 章 2 XConfig」を参照してください。新しい VP-II X ユニットのネットワークに追加した場合は必ず、そのユニットをデータベースに登録する必要があります。登録は、NetControl-X の[機器管理]メニューから手動で行うこともできます。

2.3 XAgent のセットアップ

XAgent は Windows サービスプログラムとして実行されます。XAgent はインストール時に自動的に Windows サービスに登録され、Windows が起動されると自動的に起動します。

Windows サービスとして実行される XAgent をセットアップまたは管理するために、管理ツールプログラム (XAgent Management Tool) が用意されています。このプログラムは、XAgent をインストールすると自動的にインストールされます。XAgent をセットアップするには、Windows の[スタート] > [すべてのプログラム] > [HVPR] > [XAgent]から[XAgent Management Tool]を実行します。XAgent Management Tool プログラムを終了しても、XAgent プログラムはバックグラウンドで引き続き実行されます。



上の XAgent の[サービスステータス]ウィンドウでは、手動で XAgent をスタート、ストップ、またはリスタートできます。上の例では、初期設定が実行されていないため、エラー[Can't find 'XAgent' in database](データベースに XAgent がありません)が表示されています。セットアップに進むには、[Detail]をクリックします。ウィンドウが拡張され、下のようにさらにオプションが表示されます。

□ DBMS

ここに DBMS 情報を入力する必要があります。右の例は、NetControl-X DB インストーラにより作成されたデフォルト情報です。

DBMS が同じコンピュータにインストールされている場合、デフォルト値の「127.0.0.1」をそのまま使用してください。これはローカルマシンを意味します。DBMS が別のコンピュータにインストールされている場合は、DBMS サーバの IP アドレスを入力する必要があります。

Microsoft から提供されている Microsoft SQL 2005 Management Studio Express などの SQL 管理ツールプログラムを使用して、パスワードを変更するには、[Database]および[ID]の情報はデフォルトのままにしておく必要があります。パスワードの変更後、すべての NetControl ソフトウェアコンポーネント(XAgent、NetControl-X、XConfig)に必ず同じパスワードを適用してください。変更内容をすべて確定するには[Apply]をクリックします。

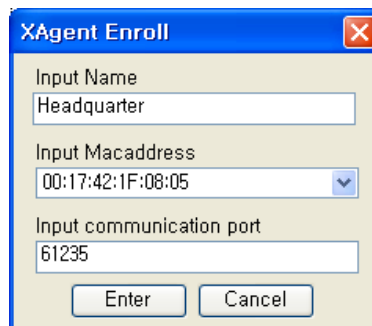
□ Master Mode Setup (マスタモード設定)

[Device Master Mode]を選択し、マスタ VP-II X ユニットの MAC アドレスを入力してから[適用]をクリックします。マスタ VP-II X ユニットが XConfig の[DB へ追加 (F2)]機能を使用して既にデータベースに登録されている場合は、右の例に示すとおり、この情報を入力する必要はありません。[Server Master Mode]を使用する場合は MAC アドレスを入力する必要はありません。

□ XAgent 登録(XAgent Enroll)

同じネットワークで稼動する XAgent はすべて DBMS に登録する必要があります。[Enroll]をクリックし、パスワードを入力して続行します。デフォルトのパスワードは「admin」です。次のウィンドウが表示されます。

NetControl-X アプリケーションに対する XAgent の名前(例:「Headquarters」、「Location A」、「New York Office」)を入力します。[Input Macaddress]は、DBMS がインストールされているサーバの物理アドレスを示します。他のアプリケーションで使用されていない限り、[Input communication port]はデフォルト値(61235)の使用をお勧めします。変更する場合は、同じポートを使用するように VP-II X ユニットすべてを変更する必要があります。



□ XAgent Input S/N

[Input S/N]は現在使用できません。これは将来のリリースで利用可能予定です。

□ XAgent サービス設定

通常、XAgent はインストール処理の途中で Windows サービスとして登録されますが、[Install]または[Uninstall]を実行して、Windows サービス(ローカル)から XAgent を登録または削除することにより、手動で制御することもできます。

□ DB Backup

2つのオプションを組み合わせて使用者のデータベースをバックアップできます。

データベースをバックアップするための設定には、作成されるファイルの数とファイルを作成する期間の 2 つがあります。作成されたファイルの数が上限に達した場合、最初に作成したファイルが削除され、新しいファイルが上書き作成されます。デフォルトでは、作成されるファイルの最大数は 6(0~999)で、期間は 1 回/月(1 回/日、1 回/週、1/月)です。

バックアップファイルの作成場所は XAgent がインストールされている場所と同じで、

C:\Program Files\HVPR\XAgent\Backup

ファイルのタイプは「tsdat」/「tsevt」が作成されます。

「tsdat」: 使用者のデータベース(静脈データ)のバックアップファイル

「tsdat」の復元(リストア)方法:

例: 20130529121609.tsdat → 20130529121609.dat

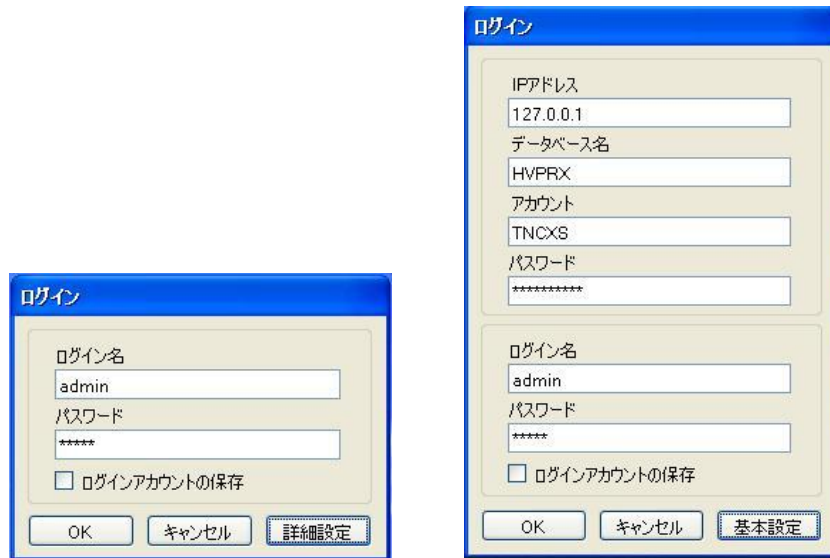
ファイルの拡張子を「tsdat」から「dat」に変更後、管理ソフトウェア「XConfig」から復元(リストア)が可能です。

「XConfig」および「XConfig」からの復元(リストア)方法については、本紙 67 頁~の「2. XConfig」をご参照ください。

「tsevt」: システムメンテナンス用の機器イベント/ログのみのバックアップファイル(使用不可)

2.4 NetControl-X へのログイン

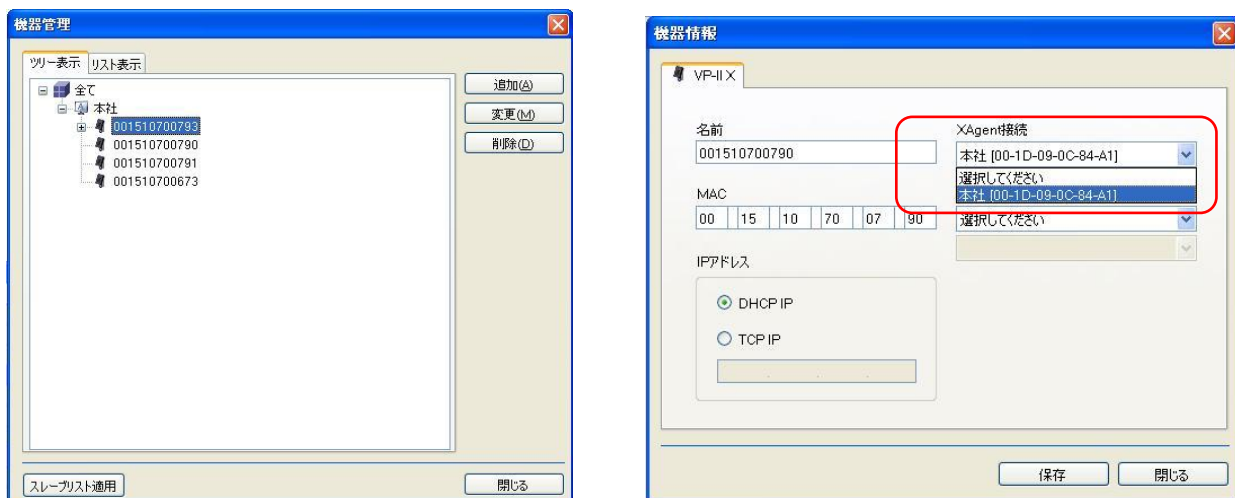
NetControl-X を起動する場合、NetControl データベース (DBMS) にログインする必要があります。初めてセットアップする場合は、[詳細設定] をクリックして、DBMS 情報を設定または確認します。DBMS がインストールされているサーバの IP アドレスを入力し、データベース名が「HVPRX」、アカウントが「TNCXS」、パスワードが「?ts2000nx!」であることを確認します。次に、[ログイン名] と [パスワード] を入力します。デフォルトでは、これらはどちらも「admin」です。NetControl-X の [ログインアカウント管理] メニューを使用して、パスワードを変更したり、異なるアクセス権を持つアカウントを追加作成したりすることができます。



2.5 VP-II X を XAgent に接続

ログイン後、NetControl-X には、DBMS に登録されている VP-II X がすべて表示されます。ここで、XAgent に VP-II X を割り当てる必要があります。これは、1 つの DBMS に複数のロケーションがネットワーク接続されている場合、異なる VP-II X グループを処理する複数の XAgent が存在する場合があるためです。

[機器] メニューの [機器管理] を選択します。VP-II X を 1 つ選択し、[変更] をクリックします。初期状態では、下の図のように VP-II X の名前は「001510700793」など MAC アドレスになっています。適宜、名前を変更し、選択された VP-II X と接続させる XAgent を [XAgent 接続] プルダウンメニューから選択してから、[保存] をクリックして適用します。



これで初期設定は完了です。システムが使用できるようになります。

2.6 パスワード管理

NetControl-X ソフトウェアで使用されるパスワードの管理には、DBMS ログイン、ネットワークパスワード、NetControl-X ログインの 3 つのカテゴリがあります。

□ DBMS

NetControl インストーラは、Microsoft SQL 2005 Express 用に管理者アカウントと使用者アカウントの両方を作成します。デフォルトでは、管理者のログイン ID は「sa」で、パスワードは「sql2005」です。また、次の使用者アカウントが作成され、NetControl-X で使用されます。

データベース名:HVPRX/アカウント名:TNCXS/パスワード:?ts2000nx!

このアカウント情報は、Microsoft SQL システムマネージャにより変更できます。XAgent、XConfig、NetControl-X が DBMS に接続できる必要があるため、アカウント情報を変更した場合は、これらのプログラムに変更した情報を適用する必要があります。

2.6.1 ネットワークパスワード

ネットワークパスワード(デフォルトでは「admin」)は XAgent と VP-II X の間で通信データを暗号化するために使用されます。また、ネットワークパスワードは XConfig を使用してネットワークパラメータを変更する場合にも入力する必要があります。このパスワードは XConfig を使用して変更できます。パスワードを変更した場合は、ネットワークに接続されている XAgent およびすべての VP-II X ユニットに適用する必要があります。

2.6.2 NetControl-X

デフォルトでは、NetControl-X のインストール時のアカウント名とパスワードは両方とも「admin」です。

3. 用語および略語

3.1 使用者のタイプ

次の表は、登録と認証に使用される ID 番号のタイプに基づく使用者のタイプとその定義をまとめたものです。

使用者のタイプ	説明
PIN 使用者	2～24 桁の使用者番号 (PIN) を使用して登録された使用者。
Prox カード使用者	Prox カードを使用して登録された使用者。 - カードの Wiegand コードが PIN として使用されます。 - 最高 128 ビットがサポートされています。
IC カード使用者	IC カード (HID iClass、MIFARE など) を使用して登録された使用者。 - 静脈データは、カードと VP-II X データベースに保存できます。
パスワード使用者	パスワードは、登録されている使用者なら誰にでも、個別に割り当てることができます。必要であれば、パスワード使用者は静脈パターンの認証を受けても受けなくても出入が許可されるようにすることができます。 - パスワードを使用して出入許可を得るには、特別な手順が必要です。詳細については、VP-II X の取扱説明書を参照してください。

3.2 管理者

管理者は、使用者の登録および削除、システム設定のセットアップまたは変更を行う権利を持つ使用者です。管理者が認証されると、ディスプレイ上に管理者メニューが自動的に表示されます。

3.3 インストーラ

インストーラは、初期導入時、VP-II X がテストモードのときに登録できる一時的な管理者です。インストーラの権限は管理者と同じであり、管理者メニューにアクセスして、使用者の登録や削除、システム設定のセットアップや変更を行えます。通常、インストーラはシステムのセットアップと設置のために一時的に管理者として登録されます。設置が完了したら、インストーラを削除することをお勧めします。インストーラの登録で使用できるのは PIN のみで、カードは使用できませんが、管理者の登録にはカードと PIN の両方が使用できます。

3.4 テストモード

テストモードは、VP-II X の工場出荷時のデフォルト設定です。テストモードでは、VP-II X を起動するたびに、インストーラを管理者として登録するためのメニューが表示されます。つまり、ユニットがテストモードである限り、電源を入れなおせば誰でも管理者として登録できることになるため、いったん設置が完了したら、システム管理者がテストモードを解除することを強くお勧めします。

3.5 セキュリティレベル

セキュリティレベルは、認証のために静脈の生体認証データを照合する際に使用される、調節可能なレベルです。レベルは 5 段階に調節できます。レベル 1 では、最も厳密に静脈データの照合が行われます。レベル (1) では照合の精度が高くなりますが、個人の静脈データの特性や環境によっては、本人拒否率も高くなる可能性があります。

工場出荷時のデフォルト設定はレベル 4 で、初めての導入ではこのレベルが推奨されます。これにより、使用者は、スキャナに対して正しい位置に立ち正しく手を入力する方法に慣れることができます。導入とトレーニングが完了したら、VP-II X のシステムレベルをレベル 3 以上に設定することをお勧めします。個人のセキュリティレベルは、固有の要件に基づいて、使用者ごとに調節することができます。

VP-II X ユニットにはそれぞれセキュリティレベル (システムレベル) が設定されています。このレベルは、各使用者のセキュリティレベル (個人のセキュリティレベル) として指定することができます。使用者を認証する場合、

VP-II X は、個人のセキュリティレベルが指定されている場合はそのレベルを、指定されていない場合はシステムレベルを使用します。

3.6 生体識別機能(HCD)レベル

VP-II X が採用している静脈パターン認証テクノロジーは、人間か人間ではない物体かを認識できます。その判断レベルを調節するには、[HCD(HCD レベル設定)]メニューを使用します。範囲は 1(最も厳密)~3、またはオフ(無効)です。

レベル 1:HCD が、最も厳密なレベルで、登録と認証の両方に適用されます。このレベルでは、人間の手のみを登録および認証できます。

レベル 2 および 3:HCD は登録にのみ適用されます。認証には適用されません。

オフ:HCD 機能は使用されません。

3.7 VP-II XG(ドアコントローラ)

VP-II X は、VP-II XG ドアコントローラを通じて、電気錠を制御できます。VP-II XG は別売りで、RS232 または RS485 経由で VP-II X に接続します(RS485 インターフェースを使用するには、VP-II X と XG の両方にオプションの RS485 ドライバボードを取り付ける必要があります)。VP-II XG には、電気錠に接続するためのリレー出力と、扉ステータスの監視および施解錠入インターフェース用デジタル入力ポートがあります。

3.8 アンチパスバック

VP-II X システムにはアンチパスバック機能が用意されています。アンチパスバックは、入室記録を持たない使用者が退室しようとしたとき、または退室記録を持たない使用者が入室しようとしたときに、出入を許可しない機能です。この機能を使用するには、入室と退室のために 2 台以上の VP-II X ユニートをグループ化する必要があります。入室に割り当てられた VP-II X ユニートで出入許可が記録された使用者のみ、退室が割り当てられた VP-II X ユニートから出入許可を得ることができます。

設定方法および使用方法の詳細については、「第 2 章 3.4 アンチパスバック機能」を参照してください。

3.9 バイパス(PIN またはカードのみの出入:静脈パターン認証なし)

バイパスは、手の甲静脈パターンの認証を行わず、PIN またはカードのみで使用者に出入許可を与える機能として定義されています。

この機能は、VP-II X のユニットごとに、または使用者ごとに設定できます。VP-II X ユニートに対してバイパス機能が有効な場合、すべての使用者は手による認証を受けずに出入許可を得ることができます。特定の使用者についてバイパスが有効な場合、この使用者は、ネットワーク上のどの VP-II X ユニートからでも、VP-II X ユニートでバイパス機能が有効であるかどうかにかかわらず、手による認証を受けずに出入許可を得ることができます。

この機能のセットアップ方法および使用方法の詳細については、「第 2 章 4.3 機器セットアップ(VP-II X のセットアップ)」を参照してください。

3.10 脅迫認証

脅迫認証オプションを使用すると、使用者が VP-II X ユニートで認証したときに緊急事態通知を生成できるようになります。脅迫認証通知を生成するには、VP-II X をある特定の手順で操作するか(VP-II X の取扱説明書を参照)、または脅迫認証が割り当てられた手で認証を受けます。右手と左手の両方を登録している使用者は、どちらかの手を脅迫認証用に割り当てることができます。割り当てられた手で認証すると、システムにより脅迫認証が生成されます。脅迫認証が行われた場合、直ちに管理者に通報するために、NetControl-X に警報通知が送信されます。また、NetControl-X は指定された使用者に宛てて、電子メールを即座に送信することもできます。また、設定によっては、Wiegand ポート経由で外部システムに脅迫警報コードを送信することもできます。

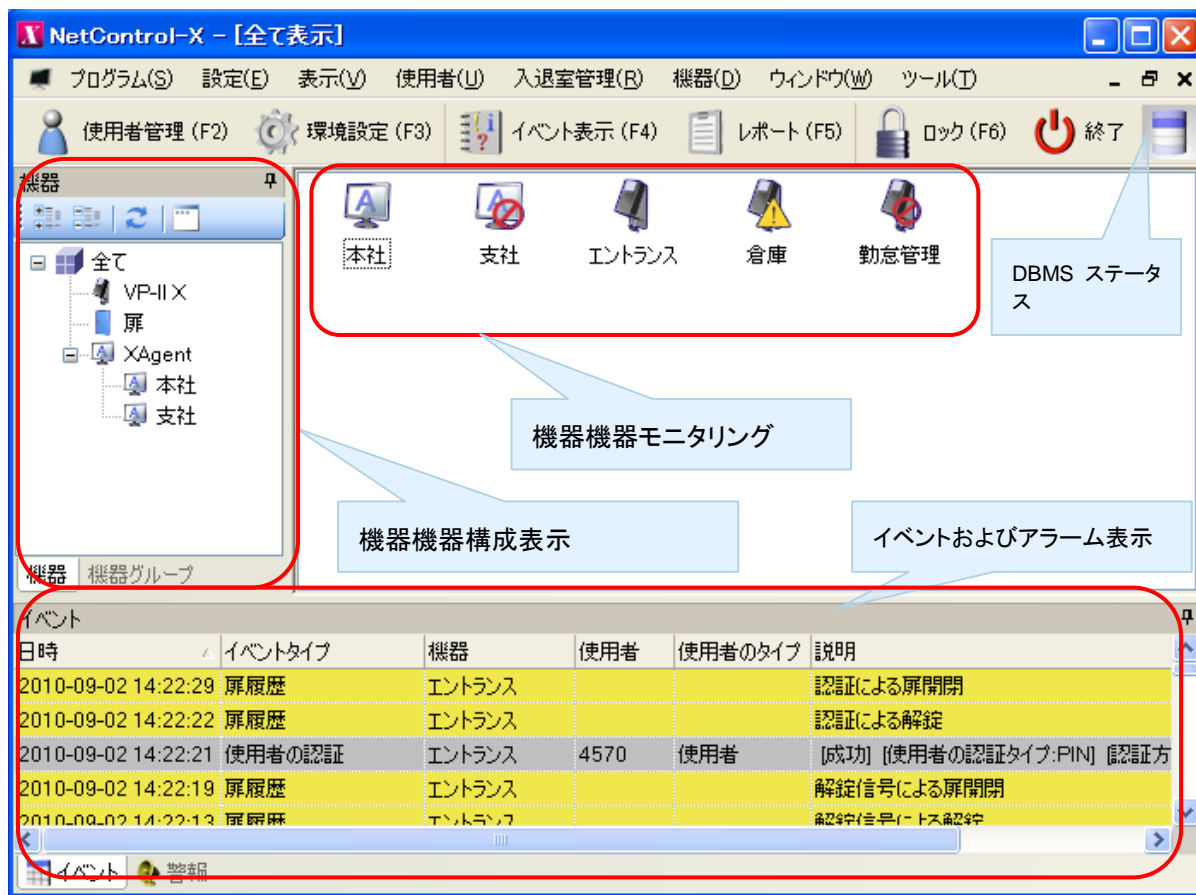
3.11 通知

VP-II X のディスプレイには従業員宛の連絡などの通知を表示することができます。通知が設定されている場合、ディスプレイの背景に通知メッセージが表示されます。「第 2 章 4.3.8 VP-II X に表示される通知」を参照してください。

第2章 NetControl-X のメニューと機能

1. メニュー

1.1 メイン画面



1.1.1 イベントおよび警報表示

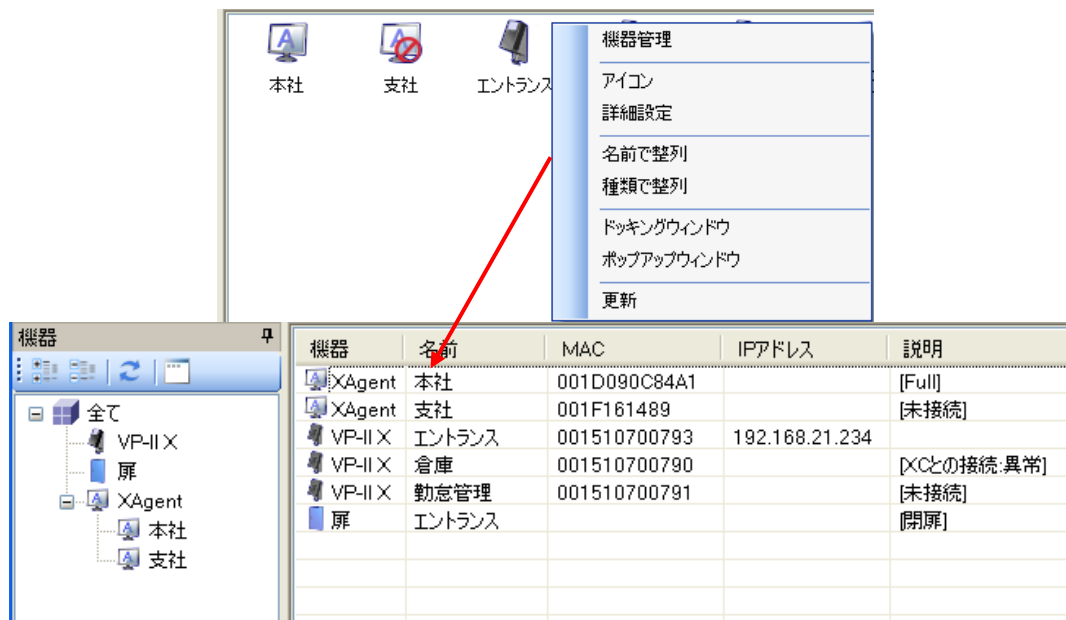
機器機器から受信したすべてのイベント(ユーザーの認証/失敗トランザクション、管理者メニューへのアクセス、システムログなど)が、イベントおよび警報表示ウィンドウに表示されます。[設定]メニューから、イベントの種類ごとに色を割り当てることができます。詳細については、「第2章 2.3 言語および表示オプション」を参照してください。

NetControl-X 画面の左下にある[警報]タブを選択すると、機器からの脅迫認証やタンパー検出などの警報メッセージがウィンドウに表示されます。警報メッセージが発生すると、[警報]タブを選択していなくても、ポップアップウィンドウにメッセージが表示されます。

1.1.2 機器モニタリング

[機器]タブが選択されている場合、機器設定表示ウィンドウには、すべての設定された機器 (VP-II X、XG、および XAgent) を含むツリーが表示されます。また、実際のマップが設定されていれば、機器がグループごとに表示されます (機器グループとマップの設定の詳細については、「第2章 4.2 機器グループ」を参照してください)。[機器グループ]タブが選択されている場合、グループが定義されていれば、グループごとに機器が表示されます。ツリーからアイテムをダブルクリックすると、選択されたアイテムに属する機器のみが表示されます。たとえば、上の図で「本社」をダブルクリックすると、本社にある XAgent に割り当てられた VP-II X と XG のみ表示されます。

機器モニタリングウィンドウには、選択された機器のステータスが表示されます。ウィンドウの空いたスペースを右クリックすると、名前、タイプ、または機器の詳細で機器を並べ替えるためのメニューが表示されます。[更新]を選択すると、機器のステータスが更新されます。



1.1.3 アイコン

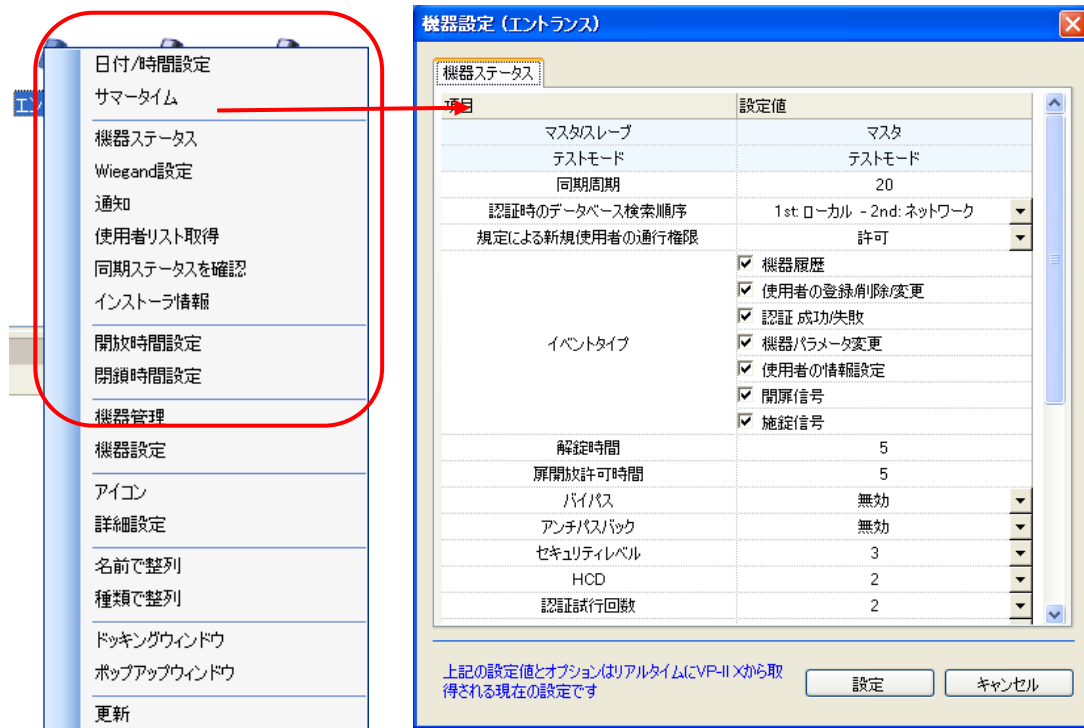
	DBMS 接続ステータス: 青(接続中) / 赤(未接続)。
	XAgent ステータス(正常 / エラー)。
	VP-II X は正常に動作しています。
	VP-II X は接続中ですが、正常に動作していません。たとえば、マスタユニットに接続できていないか、XG が使用されているときに XG コントローラと接続されていないか等。アイコンの上にマウスポインタを重ねると、エラーの詳細が表示されます。
	VP-II X エラー(未接続)。
	扉が施錠(施錠)している時。 ※XG にステータス入力が必要となります。
	扉が開扉(解錠)している時。 ※XG にステータス入力が必要となります。
	扉施錠エラー ※XG にステータス入力が必要となります。
	アイコンの背景に表示される色付きの帯には次のような意味があります。 グリーン: 開放時間帯が設定されている(開放時間帯には扉は開錠されたままです) オレンジ: バイパス機能が使用されている(使用者は静脈認証をしなくても PIN またはカードのみで出入許可を得られます) グレー: 扉閉鎖コマンドにより扉が施錠されている(このコマンドが解除されるまで、使用者が認証されても扉は開錠されません)

1.1.4 機器アイコンメニュー

機器モニタリングウィンドウで機器が正常と表示されているときに、アイコンを右クリックすると、下のようなポップアップメニューが表示されます。

下の図の赤い枠の中にある[機器設定]オプションを選択すると、セットアップウィンドウが開き、**機器からリアルタイムで取得された現在の設定が表示されます**。これらのメニューから設定やオプションの指定および変更ができます。セットアップウィンドウおよび設定の手順は、[機器設定]メニューでの手順と同じです。[使用者リスト取得]と[インストーラ情報]の機能については「第 2 章 4.5 VP-II X から使用者リストとインストーラ情報を取得」を参照してください。また、このメニューのその他の機能の詳細については、「第 2 章 4.3 機器セットアップ (VP-II X のセットアップ)」の該当セクションを参照してください。

[機器管理]メニューと[機器設定]メニューは、メインメニューにあるこれらの機能のショートカットです。これらのメニューについては、「第 2 章 4 機器管理」の該当するセクションを参照してください。




1.1.5 XAgent ステータスの確認



XAgent アイコンにエラーが表示されている場合、この XAgent に属するすべての機器は、実際には接続され機能している場合でも、切断されていると表示されることがあります。この場合、XAgent Management Tool を使用して、XAgent のステータスを確認してください。詳細は、「第 1 章 2.3 XAgent のセットアップ」を参照してください。

1.2 メニューの説明

メインメニュー	サブメニュー	機能の説明
プログラム(S)	ロック(L)	NetControl-X プログラムを Windows のシステムトレイに格納します。プログラムを再度開くには、システムトレイのアイコンをダブルクリックします。その際、ログインパスワードが必要です。 
	ログインアカウント管理(A)	「第 2 章 2.1 ログインアカウント管理」を参照してください。
	プログラム情報(I)	プログラムおよびバージョン情報を表示します。
	終了(E)	プログラムを終了します。
設定(E)	メッセージ設定(O)	メニュー名 や 表示されるメッセージなど、NetControl-X で使用される言葉を変更することができます。 「第 2 章 2.3 言語および表示オプション」を参照してください。
	祝祭日設定(H)	入退室管理のために、祝祭日および時間帯テーブルを設定します。
	時間帯テーブル設定(T)	「第 2 章 3 アクセス管理」を参照してください。
	Wiegand フォーマット設定(W)	カード使用者を対象に、Wiegand フォーマットをセットアップします。 「第 2 章 3.6 Wiegand の設定」を参照してください。
	環境設定(E)	イベント、システムログ、警報、メールによる通知に関する変更を行います。 「第 2 章 2 プログラム管理機能」を参照してください。
表示(V)	ツール 機器 機器グループ イベント 警報	メイン画面に表示する項目を選択し、表示しない項目の選択を解除します。

<p>使用者(U)</p>	<p>使用者の管理(M) 使用者の登録(E) 使用者グループ定義(G) 使用者定義可能なフィールド(C) 削除予定の使用者リスト(D) 再登録使用者リスト(R)</p>	<p>使用者を管理するための機能です。 「第 2 章 5 使用者の管理機能」を参照してください。</p>
<p>入退室管理(R)</p>	<p>アクセスエリアグループ設定(W) アンチパスバック管理(A)</p>	<p>アクセスエリアのレベルに基づいて、またはアンチパスバック制御のために、VP-II X をグループに割り当てることができます。 「第 2 章 3 アクセス管理」を参照してください。</p>
<p>機器(D)</p>	<p>機器管理(M) 機器設定(T) 機器グループ管理(G) データ同期(S)</p>	<p>これらは、VP-II X および VP-II XG ドアコントローラを管理するための機能です。機器の追加と削除、X/XG 機器すべてに対する設定またはオプションの設定ができます。 「第 2 章 4 機器管理」を参照してください。</p>
<p>ウィンドウ(W)</p>	<p>ウィンドウを重ねて表示 ウィンドウを上下に並べて表示 ウィンドウを左右に並べて表示 全て表示</p>	<p>NetControl-X のメイン画面のディスプレイレイアウトを調節することができます。</p>
<p>ツール(T)</p>	<p>イベント表示(V) レポート(R) データベースバックアップ/整理(D)</p>	<p>レポートとイベント表示の機能については、「第 2 章 6 レポート、イベント表示」を参照してください。</p>

2. プログラム管理機能

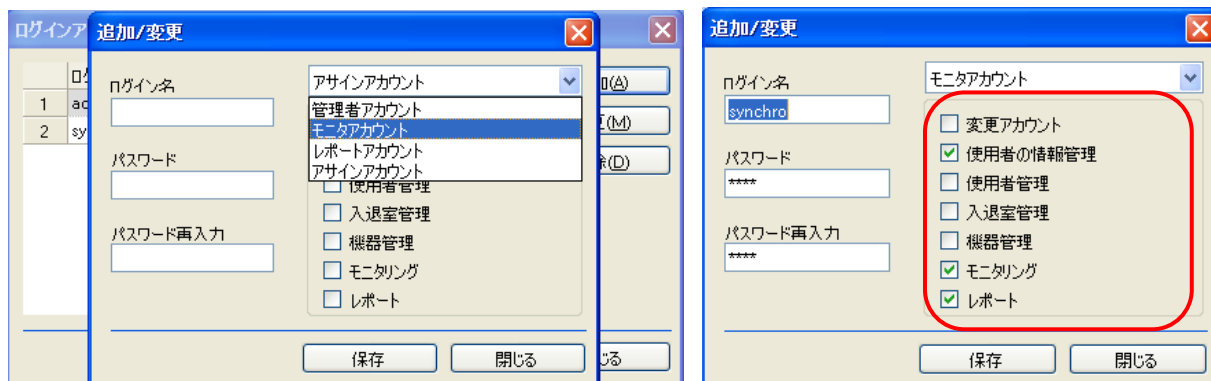
2.1 ログインアカウント管理

メニュー:[プログラム] > [ログインアカウント管理]

異なるレベルの権限を持ったログインアカウントを作成できます。アカウントのタイプに応じて、使用できるメニューは、割り当てられた機能だけに自動的に制限されます。次に説明するどの機能でも、各アカウントに割り当てることができます。また、プルダウンメニューからアカウントのタイプ(管理者アカウント、モニタアカウント、レポートアカウント)を選択した場合は、そのアカウントで使用できる機能が自動的に割り当てられます。このメニューは、管理者としてログインした場合のみ表示されます。このメニューでは、現在ログインしているアカウントのパスワードのみ変更できます。

選択できる機能は、設定アカウント、使用者の情報管理(使用者情報を表示できますが、使用者の変更や登録はできません)、使用者の管理(使用者の変更や登録が可能です)、入退室管理、機器管理、モニタリング、およびレポートです。

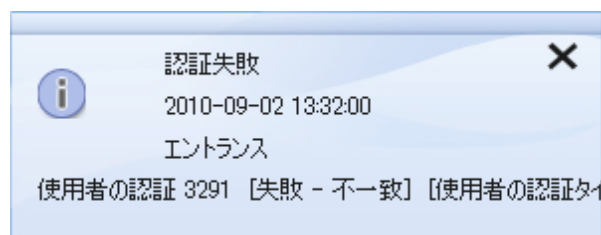
デフォルトでは、NetControl-X インストーラにより管理者アカウントが作成され、ログイン ID とパスワードが両方とも「admin」に設定されます。

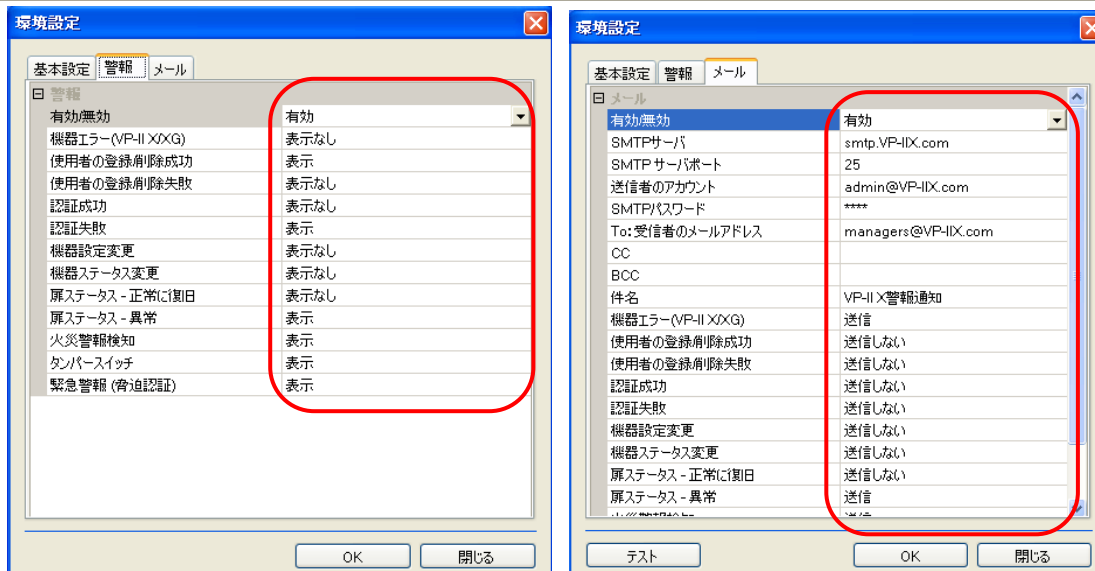


2.2 警報機能とメールによる通知

[設定] > [環境設定] > [警報]タブ/[メール]タブ

NetControl-X は、あらゆるシステムエラーやイベントに対して警報通知機能を提供しています。警報機能が有効な場合、警報が発生すると、下のようなポップアップウィンドウが Windows のデスクトップに表示されます。また、指定した受信者に警報イベントをメールで自動送信することもできます。





警報機能を使用するには、上の図に示すとおり、この機能を[有効]に設定し、使用する項目を選択([表示]または[表示なし])します。警報機能が無効であっても、これらのイベントはイベント表示ウィンドウに表示され、NetControl-X データベースに記録されます。

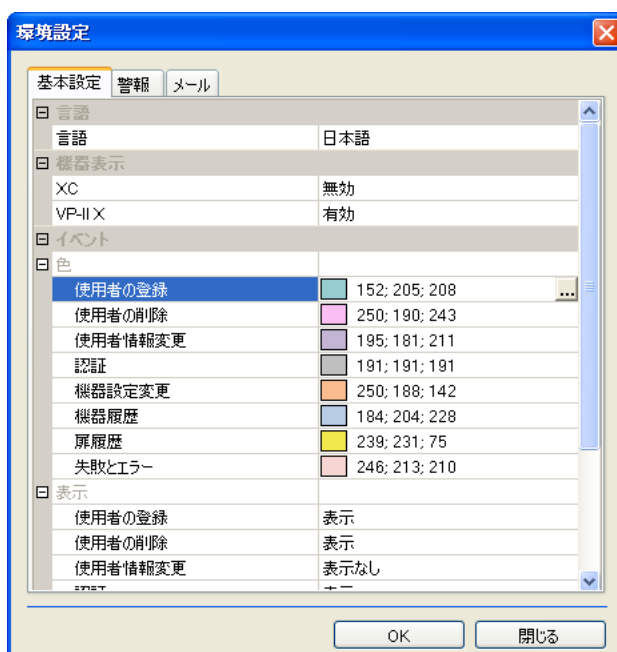
警報イベントをメールで送信するには、[メール]タブから送信を[有効]に設定し、発生したときにメール送信する項目について[送信]を選択します。[送信しない]が選択された項目に対するイベントはメールで送信されません。

送信者のメールアドレスを適切に設定する必要があります。メールを送信するとき使用するパスワード、受信者、件名などの SMTP サーバ情報を入力します。設定を有効にするには、プログラムを再起動する必要があります。

設定が正しく行われたことを確認するには、[テスト]をクリックして、メールを送信します。

2.3 言語および表示オプション

メニュー: [設定] > [環境設定] > [基本設定]タブ



□ **言語:**使用する言語を選択してください。

□ **機器表示**

VP-II X でイベントを表示するには、[有効]に設定します。[無効]に設定されている場合、イベントは表示されません。XC は将来使用される機能です。設定は[無効]のままにしておいてください。

□ **イベントの表示色**

イベントの種類ごとに異なる表示色を割り当てて、わかりやすくすることができます。変更する項目を選択して、色を割り当ててください。

□ **イベント表示オプション**

イベント監視ウィンドウに表示する必要のないイベントについては[表示なし]を選択します。選択されていないイベントでも、データベースには格納されます。デフォルトでは、すべてのイベントが表示されるように設定されています。

[失敗とエラー]という項目は、認証失敗、制限付き使用者、または何らかのシステムエラーを表示します。

2.4 メッセージの変更

必要に応じて、NetControl-X で使用されるメッセージを変更することができます。[設定] > [メッセージ設定]を選択して、[現在使用中]列にあるメッセージを変更します。変更したメッセージを有効にするには、プログラムを再起動する必要があります。

3. 入退室管理

NetControl-X と VP-II X ユニットを組み合わせることにより、あらゆる範囲の入退室管理を行うことができるようになります。使用者の出入は、時間、曜日、日付、祝祭日、ゲート(VP-II X)を柔軟に組み合わせることにより制御可能です。

祝祭日テーブルは 100 個まで、時間帯テーブルと通行許可グループテーブルは 200 個まで作成できます。また、1 つ以上のテーブルを組み合わせることで使用者に割り当てることにより、あらゆる種類のアクセス管理や制限ができます。

3.1 時間帯／エリア制限による使用者の制御

たとえば、次のような条件で使用者にアクセスを与える必要があるとします。

- (1) 月曜日から木曜日の午前 9 時から午後 5 時までのみ
- (2) 祝日には出入を許可しない
- (3) 施設内には複数のゲートがあるが、正面玄関からのみ出入を許可する

この場合、次のようにします。

- (1) その地域の祝祭日すべてを網羅した祝祭日テーブルを作成します
- (2) 開始時間が午前 9 時、終了時間が午後 5 時、有効日が月曜日から木曜日の時間帯テーブルを作成し、このテーブルに上の手順で作った祝祭日テーブルのインデックスを割り当てます。
- (3) 正面玄関だけが含まれる通行許可グループテーブルを作成し、上の手順で作った時間帯テーブルを割り当てます。
- (4) [使用者の管理]メニューを使用して、上の手順で作った通行許可グループテーブルを使用者に割り当てます。

詳細は、以下のセクションを参照してください。

3.2 時間帯制御テーブル

メニュー:[設定] > [祝祭日設定] / [時間帯テーブル設定]

時間帯テーブルは VP-II X ユニットと同期する必要があるため、マスタユニットが動作していない場合には、これらのメニューは機能しません。

3.2.1 祝祭日テーブルの設定

設定または修正するインデックス番号を 001 から 100 の範囲で選択し、テーブル名(下の例では「国民の祝日」)を入力します。次に月を選択し、その月で祝祭日に設定する日付をそれぞれクリックして、[追加]をクリックしてから、次の月を選択します。選択した日付が右側のウィンドウにリストされます。[追加]をクリックしないと、変更は反映されません。

この操作を 1 月から 12 月まで繰り返し、[設定]をクリックして保存します。[設定]をクリックすると、このテーブルのデータがマスタ VP-II X ユニットに転送されます。転送には数秒かかります。マスタユニットが動作していない場合、エラーメッセージが表示され、変更は適用されません。

祝祭日テーブルは最高 100 種類設定できるため、任意の使用者にさまざまな祝日を割り当てることができます。

祝祭日設定

祝祭日インデックス: 001
名前: 国民の祝日

September 2010

Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2

9/2/2010

日付	
1	01-01
2	01-11
3	02-11
4	03-22
5	04-29
6	05-03
7	05-04
8	05-05
9	07-19
10	09-20
11	09-23
12	10-11
13	11-03
14	11-23
15	12-23

追加 全て選択 選択解除 削除

インデックス削除 インポート/エクスポート 設定(S) 削除(D) 閉じる

3.2.2 時間帯テーブルの設定

時間帯テーブルは、次のような機能に使用します。

- **開放時間帯**: 設定された時間帯に、扉を解錠したままにします。
- **使用者時間帯**: 設定された時間帯のみ、使用者に出入が許可されます。
- **閉鎖時間帯機能**: 設定された時間帯に、扉を施錠したままにします。火災警報などの緊急時を除き、この機能が解除されるまで、使用者認証で扉を開錠することはできません。

設定または修正するインデックス番号を選択し、テーブル名を入力して、時間帯テーブルに使用する祝祭日テーブルを割り当てます。必要な[有効]/[無効]チェックボックスを選択して時間帯を設定し、[開始時間]と[終了時間]をクリックして、時間を調節します。

選択されていない曜日には、時間帯設定は適用されません。つまり、開放時間帯に対して使用した場合、選択されていない曜日には、扉は開錠されたままになりません。また、使用者時間帯に対して使用した場合、選択されていない曜日には、使用者は出入が許可されません。

祝祭日の時間帯を割り当てるには、[祝祭日インデックス]を割り当て、[祝祭日]を選択(チェック)します。次に、目的の時間帯を設定します。この時間帯は、割り当てられた祝祭日テーブルにリストされている日付の設定されている時間に対して適用されます。

複数の日付に同じ期間をまとめて設定するには、[複製]ボタンをクリックします。

時間帯テーブル設定

時間帯インデックス: 001
名前: 時間帯1
祝祭日インデックス: 無効 複製(B)

有効/無効	日	開始時間	終了時間
<input checked="" type="checkbox"/>	月	09:00	16:00
<input checked="" type="checkbox"/>	火	09:00	16:00
<input checked="" type="checkbox"/>	水	09:00	16:00
<input checked="" type="checkbox"/>	木	09:00	16:00
<input checked="" type="checkbox"/>	金	09:00	16:00
<input type="checkbox"/>	土	00:00	00:00
<input type="checkbox"/>	日	00:00	00:00
<input type="checkbox"/>	祝祭日	00:00	00:00

月 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

火

水

木

金

土

日

祝祭日

インデックス削除 インポート/エクスポート 設定(S) 削除(D) 閉じる

3.3 アクセスエリアグループ設定

メニュー:[入退室管理] > [アクセスエリアグループ設定]

また、アクセスエリアに基づいてテーブルを作成することもできます。テーブルインデックスを選択し、テーブル名を入力します。ウィンドウにはすべての機器がリストされます。次にこのグループに割り当てるゲートと、時間帯テーブルを2つまで指定します。

下の例では、ゲート「エントランス」のみが選択されています。また、時間帯テーブルのインデックス 001 と 002 (前述のセクションで作成したもの) が割り当てられています。時間帯テーブル 1 は月曜日から金曜日の午前 9 時から午後 4 時まで、テーブル 2 は月曜日から金曜日の午後 6 時から翌日の午前 1 時まで設定されているため、下の図にあるように、1 日に対して 2 つの異なる時間帯が表示されます。

このアクセスエリアグループテーブルが割り当てられた使用者は、月曜日から金曜日の午前 9 時から午後 4 時と、午後 6 時から翌日の午前 1 時までの間、エントランスからのみ出入りが許可されます。

アクセスエリアグループ設定

通行許可グループインデックス: 001

名前: エントランス

名前	IPアドレス/MAC	選択	時間帯1	時間帯2
エントランス	192.168.21.234	<input checked="" type="checkbox"/>	[001] 時間帯1	[002] 時間帯2
倉庫	00-15-10-70-07-90	<input type="checkbox"/>	無効	無効
勤怠管理	00-15-10-70-07-91	<input type="checkbox"/>	無効	無効

月 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

火

水

木

金

土

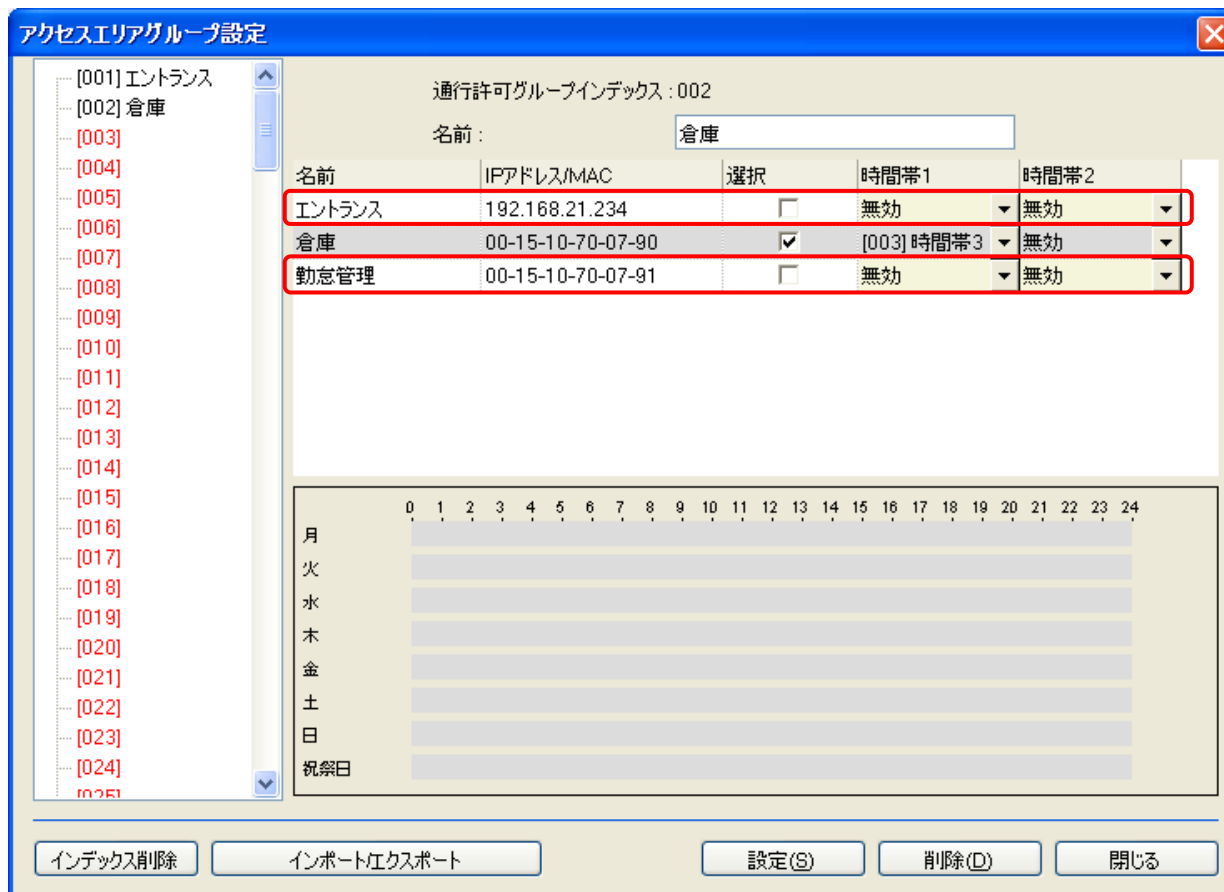
日

祝祭日

インデックス削除 インポート/エクスポート 設定(S) 削除(D) 閉じる

ゲートを選択して時間帯テーブルを割り当てなかった場合、このゲートからは常時出入が許可されます。つまり、このゲートについては、時間帯ルールは使用されません。

下の例では、アクセスエリアグループインデックス 2 が割り当てられた使用者は、エントランスゲートからは常時出入できますが、倉庫ゲートからは、時間帯テーブルインデックス 003 で設定された時間帯しか出入できません。また、サーバ室への出入は終日禁止されています。



3.4 アンチパスバック機能

アンチパスバック機能を使うよう設定されたユニットでは、アンチパスバックユニットへのアクセスを許可され、入室ユニットに入室記録が残っている使用者だけが、退室ユニットから退室許可を得ることができます。同様に、退室ユニットに退室記録が残っていない使用者(言い換えれば、退室ユニットで認証を受けずに退室した使用者)は、入室ユニットから入室許可を得ることはできません。

アンチパスバック機能を使用するには、**2 台以上の VP-II X をグループ化する必要があります**。入室用に 1 台以上、残りを退室用に使用します。複数のグループを設定して、さまざまな部屋を制御することができます。また、**VP-II X ユニットの[アンチパスバック]オプションを有効にしておく必要があります**。このオプションを有効にするには、[機器]メニューの[機器設定]を選択します。VP-II X の設定およびオプション設定の詳細については、「第 2 章 4.3 機器設定(VP-II X の設定)」を参照してください。

NetControl-X でアンチパスバック機能を設定するには、次のようにメニューを選択します。

メニュー:[入退室管理] > [アンチパスバック管理]

[アンチパスバック管理]ウィンドウが表示されたら、[追加]または[変更]ボタンをクリックして、入室用または退室用のアンチパスバックユニットをグループ化します。アンチパスバック使用者を割り当てるには、リストからグループ名を1つ選択し、[アンチパスバック情報]ボタンをクリックします。

右側のウィンドウから少なくとも2つのVP-II Xユニット(グループ化するもの)を選択し、[<<]ボタンをクリックして、左側のウィンドウに移します。次に、各ユニットに[入室]または[退室]を割り当てます。アンチパスバック機能を使用するには、少なくとも入室用ユニットが1つと、退室用ユニットが1つが必要です。この機能を一定の時間帯だけ使用する場合は、[開始時間]と[終了時間]を設定します。

アンチパスバック管理

名前: テスト

名前	IPアドレス/MAC	入室/退室
1 エントランス	192.168.21.234	入室
2 倉庫	00-15-10-70-07-90	退室

開始時間: 2010-09-02 00:00

終了時間: 2010-09-02 14:47

保存 キャンセル

名前	IPアドレス/MAC
1 勤怠管理	00-15-10-70-07-91

アンチパスバック情報

★ 使用者の追加(A) ● 使用者の変更(M) ✖ 使用者の削除(D) ↻ 更新(R) ✕ 閉じる(X)

- 入室
 - エントランス
- 退室
 - 倉庫

PINタイプ	PIN	名前	開始時間	終了時間	ステータス
PIN	3291		2010-09-02 14:48		入室
PIN	4570		2010-09-02 14:48		退室

[使用者追加]をクリックすると、登録されている使用者の一覧が表示されます。割り当てる使用者を選択します。また、割り当てられた使用者に許可する時間帯を設定するには[使用者変更]メニューを使用します。

上の図には、入室および退室を行った使用者の現在のステータスが表示されています。「入室」は、使用者は入室用ユニットを通過して入室したが、退出用ユニットを通過して退出していない、つまりこの使用者はまだ施設の中にいることを表します。ステータスに「入室」と表示されているが、すでに退室している(手の甲認証を受けずに、誰かの後をついて出て行った)場合、この使用者は入室ユニットを通過して入室することは許可されません。もう一度、入室ユニットを使用できるようにするには、このメニューからステータスを「退室」に手動で変更する必要があります。

退室ユニットでは時間帯機能を使用しないことをお勧めします。退室ユニットに時間帯を使用すると、万が一、使用者が設定された時間よりも遅くまで施設内にとどまっていた場合、部屋に閉じ込められてしまう可能性があります。

3.5 扉管理機能

VP-II XG ドアコントローラを使用している場合、扉管理機能を使用できます。扉管理機能の詳細については、「第 2 章 4.3 機器セットアップ (VP-II X のセットアップ)」を参照してください。

3.6 Wiegand の設定

3.6.1 Wiegand フォーマット設定

メニュー:[設定] > [Wiegand フォーマット設定]

システムで使用される Wiegand フォーマットを設定します。総ビット長とサイトコード(ファシリティコード)のビット長を設定します。NetControl は、奇数パリティビットと偶数パリティビットを 1 ビットずつとみなし、残りのビットをカードシリアル番号(CSN)に使用します。26 ビットの Wiegand コードを例にすると、サイトコードのビット長を 8 とした場合、CSN のビット長は 16 になります(奇数パリティ 1 ビット+サイトコード 8 ビット+ CSN 16 ビット+偶数パリティ 1 ビット)。

総ビット長	サイトコードビット長
26	8
27	0
28	0
29	0
30	0
31	0
32	0
33	0
34	12
35	0
36	0
37	0

表示オプション
 カードシリアル番号

区切り文字
 :

保存 閉じる

Wiegand フォーマットが設定されると、カード使用者のカード番号は、定義されたカードフォーマットに従って管理され、選択された表示オプションに従って表示されます。上の図に示すように、プルダウンメニューから表示オプションを選択します。また、表示のときに、Wiegand ビット、サイトコード、CSN の区切りに使用する区切り文字も入力します。

たとえば、Wiegand データが 26 ビット **00001111100101011101001100** のカードでは、サイトコードと CSN は次のようになります。

	総 Wiegand ビット数	奇数パリティ (1 ビット)	サイトコード(8 ビット)	CSN(16 ビット)	偶数パリティ (1 ビット)
2 進数		0	00011111	0010101110100110	0
10 進数	26		31	11174	

[カードシリアル番号]が選択されている場合、次のように表示されます。複数のタイプの Wiegand フォーマットやサイトコードが使用されている場合、次の例に示すように、その数値が PIN として表示されることがあります。

User Type	PIN	First Name	Last Name	Employee ID
Prox. Card User	11174	David	Johnson	22222
Prox. Card User	11175	Alex	Hollywood	
Prox. Card User	11175			

[サイトコード+カードシリアル番号]が選択されている場合は、次のように表示されます。

User Type	PIN	First Name	Last Name	Employee ID
Prox. Card User	31:11174	David	Johnson	2222
Prox. Card User	31:11175	Alex	Hollywood	
Prox. Card User	32:11175			

[Wiegand ビット+サイトコード+カードシリアル番号]が選択されている場合は、次のように表示されます。

User Type	PIN	First Name	Last Name	Employee ID
Prox. Card User	26:31:11174	David	Johnson	2222
Prox. Card User	26:31:11175	Alex	Hollywood	
Prox. Card User	26:32:11175			

□ 未定義の Wiegand フォーマットの表示

Wiegand フォーマットが定義されていないカードを使って使用者を登録した場合、そのカード番号は「1A0F95D33FFFFFF」のように 16 進数コードで表示されます。これは目で見て確認できません。この 16 進数コードにはオリジナルの Wiegand データが含まれます。先頭バイトは Wiegand データの総ビット長を示します。2 バイト目からがオリジナルの Wiegand データです。

オリジナルの Wiegand データの先頭ビットは、通常偶数パリティビットですが、2 バイト目 (バイト 2) の MSB になり、8 ビット目が LSB になります。同様に、9 ビット目がバイト 3 の MSB になります。使用されていないビットには「1」が入ります。

バイト 1	バイト 2	バイト 3	~	バイト 7
Wiegand の総ビット数	先頭 8 ビット (ビット 0~7)	ビット 8~15	~	~

たとえば、Wiegand データが 26 ビット **00001111100101011101001100** のカードでは、16 進数の Wiegand コードは 1A0F95D33FFFFFF です。

	バイト 1	バイト 2	バイト 3	バイト 4	バイト 5	バイト 6	バイト 7
2 進数	00011010	00001111	10010101	11010011	00111111	11111111	11111111
16 進数	1A	0F	95	D3	3F	FF	FF

前述のメニューを使用して適切な Wiegand フォーマットが定義されるまで、16 進数の Wiegand コードが PIN として管理されます。

3.6.2 VP-II X Wiegand 出力の設定

メニュー:[機器] > [機器設定] > [Wiegand]タブ

このメニューを実行すると、NetControl-X は選択した VP-II X から設定をリアルタイムで受け取り、現在の設定値を表示します。目的の項目を修正し、[設定]をクリックして、VP-II X に適用します。

設定	項目	設定値
<input type="checkbox"/>	総ビット長	26
<input type="checkbox"/>	サイトコードビット長	8
<input type="checkbox"/>	パルス幅(PWT)	40
<input type="checkbox"/>	パルス間隔(PIT)	2000
<input type="checkbox"/>	サイトコード - 認証成功	0
<input type="checkbox"/>	サイトコード - 認証失敗	0
<input type="checkbox"/>	サイトコード - 脅迫認証	0
<input checked="" type="checkbox"/>	Wiegand 出力タイプ	<input checked="" type="checkbox"/> 成功 <input type="checkbox"/> 失敗 <input type="checkbox"/> 脅迫
<input type="checkbox"/>	1000Card	無効

上記の設定値またはオプションは出荷時設定でVP-II Xの現在の設定ではありません

設定 キャンセル

□ パルス幅の時間／パルス間隔の時間

これらは Wiegand 信号の物理特性を示します。特定の用途で必要とされない限り、これらの値は変更しないでください。変更すると、外部システムとの通信に問題が発生する可能性があります。

□ 総ビット長／サイトコードビット長／認証成功時のサイトコード

使用者が正常に認証されると、VP-II X は他入退室管理システムとの連携のために Wiegand コードを出力します。(1)カード使用者に対しては、カードから読み取られた Wiegand コード、(2)PIN 使用者に対しては、あらかじめ設定されたフォーマットに従って作成された Wiegand コードが出力されます。

PIN 使用者に対して、Wiegand フォーマットと、認証の成功に対するサイトコード値(0~255)を設定し、[Wiegand 出カタイプ]で[成功]を選択する必要があります。カード使用者の場合、カードから読み取られた Wiegand コードが他入退室管理システム(PACS)に直接渡されるため、ここで設定されたサイトコードは影響しません。

□ Wiegand 出カタイプ

VP-II X は、認証失敗と緊急事態通報(脅迫認証)についても Wiegand コードを出力できます。他入退室管理システム(PACS)にこれらのコードの違いを認識させるには、使用するチェックボックス([認証失敗]または[脅迫認証])を選択し、異なるサイトコード値(0~255)を入力します。

認証失敗または脅迫認証の場合、PIN 使用者とカード使用者の両方について、オリジナルの Wiegand コードのサイトコードがこの値で置き換えられます。

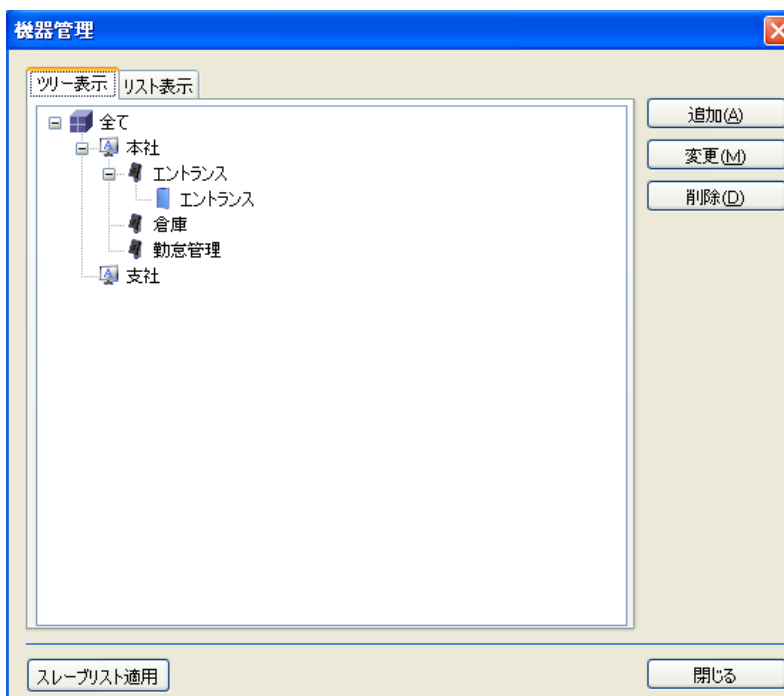
受信側他入退室管理システム(PACS)も、異なるサイトコードを認識できるように適切に設定しておく必要があります。

4. 機器管理

4.1 追加／削除(VP-II X、XAgent、XG)

VP-II X、XAgent、または VP-II XG ドアコントローラをネットワークに追加する、またはネットワークから削除する場合は、[機器管理]メニューを使用します。

メニュー:[機器] > [機器管理]



XAgents はすべて、VP-II X とともに表示されます。また、VP-II XG ドアコントローラを通じて VP-II X に接続されている扉があれば、その扉もともに表示されます。新規に追加する場合は[追加]をクリックします。次の情報の入力または設定が必要です。

□ XAgent

名前、XAgent が稼動しているサーバの MAC アドレス、および TCP/IP コミュニケーションポート(デフォルトでは 61235。別のアプリケーションで使用されていない限り、ポート番号はデフォルトのままにしておくことをお勧めします)を指定します。

XAgent Management Tool を使用して XAgent を追加することもできます。詳細については、「第 1 章 2.3 XAgent のセットアップ」を参照してください。

□ VP-II X

名前、MAC アドレス、IP アドレス(DHCP ではなく固定 IP が使用されている場合)を指定し、接続する XAgent を割り当てます(詳細については、「第 1 章 2.5 Link VP-II X を XAgent にリンク」を参照してください)。 [XC 接続]オプションは現在使用できませんので無視してください。

VP-II X の追加には、XConfig ツールを使用します。詳細については、「第 3 章 2 XConfig」を参照してください。

□ 扉(VP-II XG)

これは VP-II X に VP-II XG ドアコントローラを追加するために使用します。XG が接続されている場合は、それを指定し、XG 経由で扉を接続する VP-II X を割り当てます。

変更する場合は、目的の機器を選択し、[変更]をクリックします。

4.2 機器グループ

1 つのネットワークで多数のユニットを使用している場合は、メイン画面で簡単に監視できるように、機器をグループ化することができます。グループ化された機器は、[機器モニタリング]ウィンドウで、グループごとに表示することもでき、すべて表示することもできます。

メニュー:[機器] > [機器グループ管理]

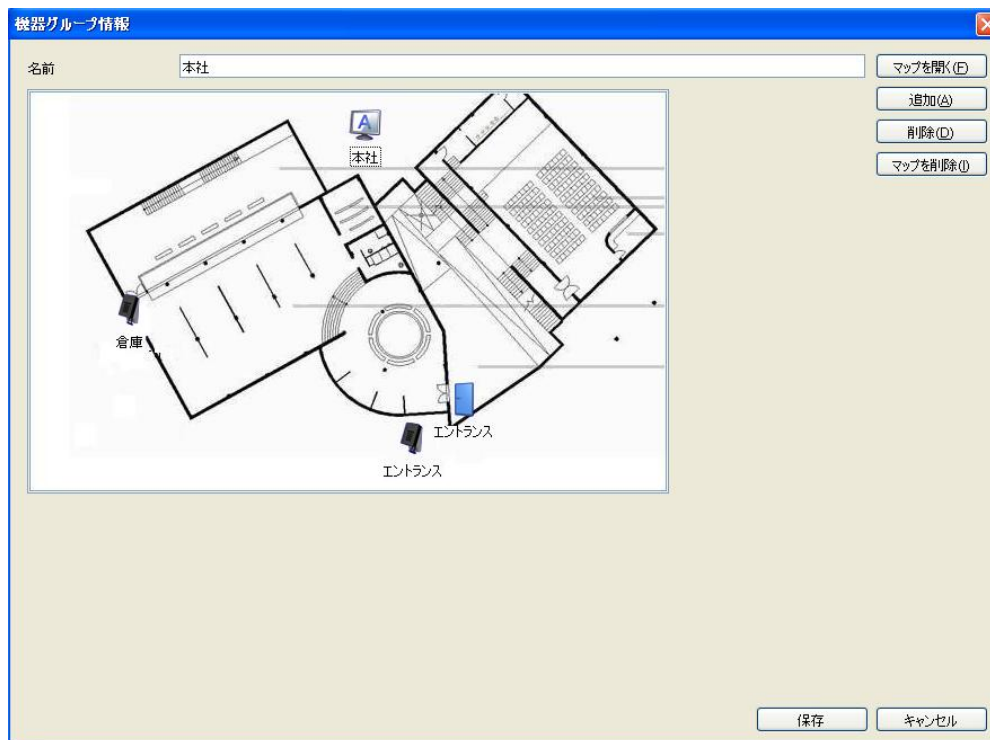
4.2.1 機器のグループ化

[機器グループ管理]ウィンドウが表示されたら、[追加]または[変更]ボタンをクリックします。次のウィンドウが表示されます。

作成するグループの名前を入力し、[追加]をクリックします。機器リストが表示されます。初期状態では、ネットワークで現在設定されている機器(XAgents、VP-II X、および扉)がすべて表示されますが、別のグループに割り当てられた機器は表示されません。編集中のグループに追加する機器を選択します。上の例では、「本社」という名前の下に、XAgent が 1 つ、VP-II X が 2 台、扉が 2 つグループ化されています。[保存]をクリックして適用します。

4.2.2 マップの割り当て

NetControl-X には、機器が実際にある場所を示したマップを使用して機器を監視し制御する機能が用意されています。機器グループ 1 つにつきマップを 1 つ割り当てることができます。下の例に示すように、[マップを開く]をクリックして、JPG または BMP 形式のマップイメージをロードし、このマップ上で、実際の環境で機器が取り付けられている場所に機器を配置(ドラッグしてドロップ)します。[保存]をクリックして適用します。



マップを使って機器を監視するには、メイン画面で[機器グループ]タブを選択します。

NetControl-X - [本社]

プログラム(S) 設定(E) 表示(V) 使用者(U) 入退室管理(R) 機器(D) ウィンドウ(W) ツール(T)

使用者管理 (F2) 環境設定 (F3) イベント表示 (F4) レポート (F5) ロック (F6) 終了

機器グループ

- 全て
- 本社

機器 機器グループ

イベント

日時	イベントタイプ	機器	使用者	使用者のタイプ	説明
[Empty event log table]					

イベント 警報

4.3 機器設定 (VP-II X の設定)

VP-II X のパラメータや設定は一部を除き、NetControl-X で、次のメニューを使って設定または変更できます。現在ネットワークで設定されている VP-II X ユニットがすべてリストされます。

メニュー: [機器] > [機器設定]

[機器設定] ウィンドウが表示されたら、VP-II X を 1 台以上選択し、[設定] をクリックします。次のウィンドウが表示されます。このメニューには 6 つのタブがあります。設定する項目のタブをクリックします。

この設定ウィンドウに表示されている設定値やオプションは工場出荷時のデフォルトです。現在の VP-II X の設定ではありません。これは、複数の VP-II X ユニートを一度に選択して設定を複製できるようにするためです。

VP-II X の現在の設定を表示するには、メイン画面の機器モニタリングウィンドウで目的の機器アイコンを右クリックします。この機能については、「第 2 章 1.1.4 機器アイコンメニュー」を参照してください。

機器設定 (エントランス)

機器ステータス 日付時刻 サマータイム Wiegand 開放時間 閉鎖時間 テストモード

設定	項目	設定値
<input type="checkbox"/>	日付時刻設定オプション	ローカル設定保持 (機器固有の時間)
<input type="checkbox"/>	認証時のデータベース検索順序	1st: ネットワーク - 2nd: ローカル
<input type="checkbox"/>	規定による新規使用者の通行権限	許可
<input type="checkbox"/>	イベントタイプ	<input checked="" type="checkbox"/> 機器履歴 <input checked="" type="checkbox"/> 使用者の登録/削除/変更 <input checked="" type="checkbox"/> 認証 成功/失敗 <input checked="" type="checkbox"/> 機器パラメータ変更 <input checked="" type="checkbox"/> 使用者の情報設定 <input checked="" type="checkbox"/> 開扉信号 <input checked="" type="checkbox"/> 施錠信号
<input type="checkbox"/>	解錠時間	5
<input type="checkbox"/>	扉開放許可時間	0
<input type="checkbox"/>	バイパス	無効
<input type="checkbox"/>	アンチパスバック	無効
<input type="checkbox"/>	セキュリティレベル	3
<input type="checkbox"/>	HCD	1
<input type="checkbox"/>	認証試行回数	2
<input type="checkbox"/>	言語	韓国語
<input type="checkbox"/>	キーボード使用	有効

上記の設定値またはオプションは出荷時設定でVP-II X の現在の設定ではありません

設定 キャンセル

設定したい項目の左側にあるチェックボックスをオンにし、[設定値] に値またはオプションを設定します。次に、[設定] をクリックして適用してから、次のタブに移ります。選択した (チェックボックスをオンにした) 項目に対する変更は、リアルタイムで VP-II X ユニットに送信されます。すべてのユニットを更新するために必要な時間は、一

度に選択したユニットの数によって変わります。選択されなかった VP-II X ユニットの更新されず、以前の設定がそのまま保持されます。

4.3.1 機器ステータス

下のパラメータは、オプションの設定です。下の表にある項目の操作や意味について、詳細は『VP-II X 取扱説明書』で管理者メニューの説明を参照してください。

□ 規定による新規使用者の通行権限

新規登録された使用者については、NetControl-X の管理機能を使って時間帯やアクセスエリアの割り当てなど適切な出入規則が設定されるまで、出入許可を制限することができます。このオプションを使用するには[制限]を選択します。

[許可]を選択すると、新規登録された使用者はすべて、登録と同時にネットワーク上のすべてのユニットにアクセスできるようになります。後で、出入規則を適用した適切な管理が必要になる可能性があります。

□ バイパス

[有効]が選択されている場合、使用者は、静脈認証をしなくても、PIN またはカードのみで出入許可を得ることができます。バイパス操作の詳細については、「第 1 章 3.9 バイパス (PIN またはカードのみの出入: 静脈パターン認証なし)」を参照してください。

□ アンチパニック

アンチパニック機能を使用するには、このオプションで[有効]を選択する必要があります。この機能の使用方法については、「第 2 章 3.4 アンチパニック機能」を参照してください。

同期期間	マスタとスレーブの間での同期間隔
日付/時間設定オプション	ローカル設定保持: 時刻は独立で、サーバに合わせられません。 タイムサーバによる自動時刻調整: VP-II X は日付と時刻を DBMS サーバに定期的に合わせます。
認証時のデータベース検索順序	最初にローカルを検索して次にネットワークを検索する、その逆、ローカルのみ、ネットワークのみのオプションがあります。
イベント種類	レポートするイベントの種類を選択します。選択されていないイベントはサーバにレポートされません。
解錠時間	認証に成功した場合に扉解錠信号をアクティブにする時間 (0 ~ 255 秒)。
扉開放許可時間	VP-II XG が解錠信号を発信した時点から扉を開けたままにしておくことができる最大時間。設定された時間内に扉が閉じられなかった場合、警報が発生します。
セキュリティレベル、HCD、 認証試行回数、キーパッド使用、音量、スリープまでの時間、 タンパースイッチ、言語、 GMT 情報	『VP-II X 取扱説明書』に従って適宜設定します。
機能キーによる解錠	必要に応じて、VP-II X は、使用者が機能キーを入力して認証されたときに解錠信号を生成できます。各機能キーを必要に応じて選択または選択解除してください。

	たとえば、このメニューで F1 を選択しなかった場合、使用者が PIN を入力する前に F1 を押すと、VP-II X はこの使用者の認証が成功しても扉を解錠しません。
--	--------------------------------------------------------------------------------------

4.3.2 日付／時間設定

[日付／時間]タブに進み、[データベース時間]または[マニュアル設定]を選択して、[設定]をクリックし適用します。これはすぐに適用されます。

時間を正確に保つには、[タイムサーバによる自動時刻調整]オプションを有効にします。これにより、VP-II X は DBMS サーバを使って毎日日付と時刻を自動調整します。時刻調整を実行するために時刻を設定するには、[機器] > [データ同期] > [日付／時間]タブを使用します。

4.3.3 サマータイム

サマータイムが自動的に設定されるようにするには、VP-II X でサマータイムの開始時間と終了時間を設定する必要があります。いったん設定すれば、VP-II X の時刻は期間の設定に基づいて自動的に調整されます。

4.3.4 Wiegand

「第 2 章 3.6.2 VP-II X Wiegand 出力の設定」を参照してください。

4.3.5 開放時間帯

設定された期間、VP-II X で、扉を解錠したままにしておく開放時間帯を設定します。この機能は、VP-II XG ドアコントローラを使用している場合に利用できます。

開放時間帯を手動で設定することはできません。プルダウンリストからあらかじめ定義された時間帯テーブルを割り当てます。時間帯テーブルの定義方法については、「第 2 章 3.2.2 時間帯テーブルの設定」を参照してください。

下部にあるオプション[運用タイプ]では、設定された開始時間から扉を開錠したままにするか([すぐに適用]を選択)、開始時間後、最初の使用者が認証され、開錠されるまで待つか([使用者の認証後に適用]を選択)を選択します。

4.3.6 閉鎖時間帯

VP-II X は設定された期間、扉を施錠したままにし、正常に認証されても、すべての使用者に対して扉の解錠を許可しません。ただし、火災警報が検知された場合、扉は自動的に解錠されます。

開放時間帯と同様、あらかじめ定義された時間帯テーブルを割り当てます。時間帯テーブルの定義方法については、「第 2 章 3.2.2 時間帯テーブルの設定」を参照してください。

4.3.7 テストモード

重要: テストモードを解除する前に、「第 1 章 3.4 テストモード」を参照して、テストモードの詳細について理解しておいてください。

[テストモード解除(復旧可能)]を選択すると、テストモードは解除されますが、システム管理者は VP-II X の管理者メニューからテストモードに戻すことができます。

[テストモード解除(復旧不可能)]を選択して、テストモードを完全に解除した場合、ユニットを工場に送り返さないかぎり、テストモードに戻すことはできません。

4.3.8 VP-II X に表示される通知

VP-II X の LCD 画面には次のように通知メッセージを表示することができます。



この機能を使用するには、下の図に示すように[表示有効]を選択し、それぞれの行のメッセージを設定します。最大 5 行設定できます。VP-II X での表示に使用される文字サイズは、指定されたメッセージが 1 行に入るように自動調整されます。また、各行の色を設定することもできます。



4.4 データベース同期

メニュー:[機器] > [データ同期]

データ同期コマンドを手動で実行するには[同期]をクリックします。このコマンドはマスタユニットに送信され、マスタユニットとスレーブユニットが自動的に同期されます。

デフォルトでは、同期機能はマスタユニットにより定期的に自動実行されるか、使用者の新規登録や削除などデータベース情報が変更されたときに自動実行されます。

このメニューでは、日付/時刻調整機能の実行時刻を設定することもできます。VP-II X は毎日、このメニューで設定された時刻に日付と時刻を DBMS サーバと合わせます。

4.5 VP-II X から使用者リストとインストーラ情報を取得

メイン画面で、ステータスが正常と表示されている VP-II X のアイコンを右クリックすると、使用者リストやインストーラ情報を取得できます。VP-II X が動作していない場合、このメニューは利用できません。

□ 使用者リスト取得

すべての使用者の PIN またはカード番号および使用者タイプ(使用者または管理者)が VP-II X から取得され、リストされます。また、使用者や時間帯テーブルなどの制御テーブルの同期ステータスも表示されます。

□ インストーラ情報

インストーラは、取り付けと初期設定のために、VP-II X がテストモードである間のみ、各 VP-II X ユニットに登録できる一時的な管理者です。初期設定とトレーニングが完了したら、インストーラを削除することを強くお勧めします。

このメニューには、インストーラ ID(PIN)があれば表示され、削除することができます。

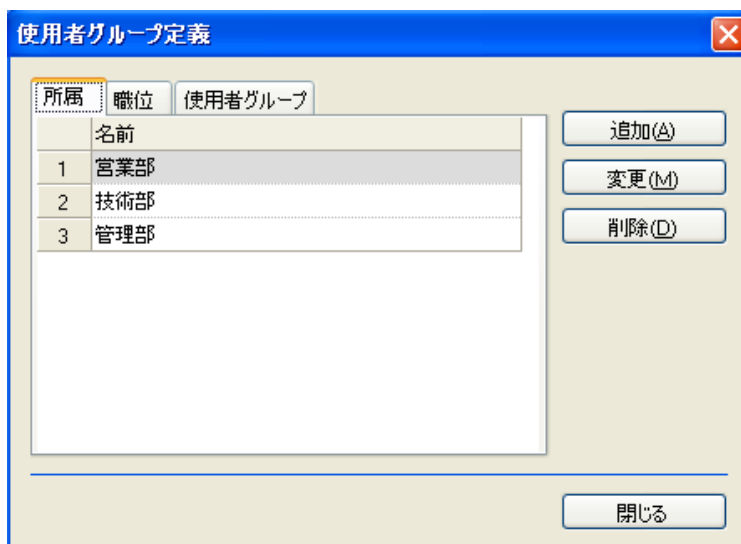
5. 使用者管理

5.1 使用者グループ定義

メニュー:[使用者] > [使用者グループ定義]

このメニューを使用して、所属、職位、使用者グループなどで使用者グループを定義し、検索、使用者情報の一括設定、レポートの生成などの管理をしやすくなることができます。

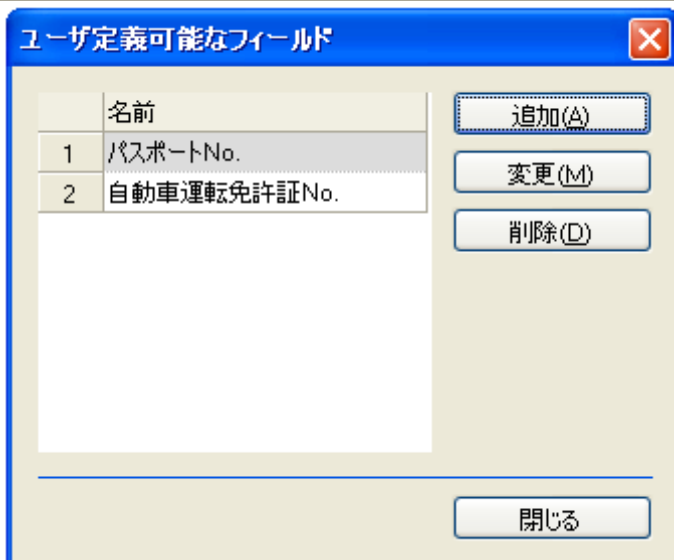
グループは、所属別、職位別、使用者グループ別に作成します。下の例には所属別に営業部、技術部、管理部の 3 つの使用者グループがあります。[使用者グループ]タブは、たとえば、支社 A、支社 B、支社 C など、所在地別に使用者をグループ化するために使用できます。



5.2 使用者定義可能なフィールド

メニュー:[使用者] > [使用者定義可能なフィールド]

名前や社員 ID などデフォルトの使用者情報フィールドに加えて、運転免許証番号などの必要な情報フィールドを無制限に作成して追加できます。



5.3 使用者の登録

メニュー:[使用者] > [使用者の登録]

使用者登録を進めるには、マスタユニットが動作していなければなりません。

これは新規使用者を登録するためのメニューです。登録済み使用者の使用者情報を変更したり、事前登録使用者の静脈データを登録したりするには、[使用者の変更]を使用します。詳細は後述のセクション「第 2 章 5.5 使用者変更」を参照してください。

新規使用者を登録するには、[認証方法]([PIN]または[カード])を選択します。[PIN]を選択した場合は、PIN を入力します。次に、登録に使用する VP-II X 機器を選択します。また、使用者の名前と社員 ID の他、[詳細設定]ボタンをクリックすることにより、所属、職位、セキュリティレベル、通行許可グループ、有効期限、認証方法などの使用者情報を入力することもできます。

□ **ユーザータイプ: 使用者／管理者**

□ **有効／無効**

[無効]を選択すると、静脈データを含むすべてのユーザー情報がデータベースに保存されていても、使用者は出入許可を得られません。出入許可を得られるようにするには、このオプションを[有効]に設定する必要があります。

□ **バイパス**

このオプションで[有効]が選択されている場合、使用者は手の甲の静脈認証を受けなくても、PIN またはカードを使用するだけで、このネットワークのすべてのユニットで出入許可を得ることができます。

□ **脅迫認証**

脅迫認証操作については、「第 1 章 3.10 脅迫認証」を参照してください。

□ **有効時間／有効期限**

これらの項目を設定して、使用者の有効時間や有効期限を設定することができます。有効期限を過ぎてしまっても、この設定を調整することにより、後で再度有効化することができます。静脈データを再登録したり、使用者情報を再入力したりする必要はありません。

□ **通行許可グループ**

論理的に通行許可エリアを制限するには、通行許可グループを割り当てます。デフォルトは[選択してください]で、使用者は登録されていればすべてのエリアに出入することができます。使用者が通行できるエリアを制限するには、「3.3 通行許可エリアグループテーブル」の手順に従ってエリアを設定し、このメニューで選択する必要があります。

□ **登録機**

錠アイコン左のチェックボックスにチェックを入れることで登録機となる VP-II X を登録時に都度、選択しないで登録機として固定することができます。

5.4 [使用者管理]メニュー

メニュー:[使用者] > [使用者管理]

このメニューから使用者を登録、変更、削除、インポートまたはエクスポートできます。

左側のウィンドウから1つの使用者グループまたはすべての使用者を選択し、PIN や名前を入力して、入力した文字を含む PIN または名前を持つ使用者をすべて検索します。たとえば、[PIN]フィールドに「1」だけを入力すると、いずれかの桁に「1」が含まれる PIN を持つ使用者がすべて表示されます。[全て検索]をクリックすると、すべての使用者をリストアップします。また、[詳細検索]をクリックすると、所属、使用者グループ、セキュリティレベル、有効期限、カスタム定義などの詳細条件を使って、使用者を検索できます。使用者の検索には、類似した語句や完全に一致する語句など、さまざまな情報を使用できます。

各メニューの機能の詳細については、以下のセクションを参照してください。[使用者登録]メニューでは、[使用者] > [使用者登録]メニューで表示されるウィンドウと同じ使用者登録ウィンドウが表示されます。この機能については、「第2章 5.3 使用者登録」を参照してください。

	PIN	PINタイプ	PIN	名前	社員ID	所属	職位	使用者グループ	セキュリティレベル	使用者のタイプ	登録日
1	PIN	007						2		管理者	2010
2	PIN	0221						スキャナレベル		使用者	2010
3	PIN	11						スキャナレベル		使用者	2010
4	PIN	13				営業部	マネージャー	スキャナレベル		使用者	2010
5	PIN	16						スキャナレベル		使用者	2010
6	カード	1793306731						スキャナレベル		管理者	2010
7	PIN	3291						スキャナレベル		使用者	2010
8	カード	3395269034						スキャナレベル		使用者	2010
9	PIN	4570						スキャナレベル		使用者	2010
10	PIN	67				技術部		スキャナレベル		管理者	2010
11	PIN	71						スキャナレベル		使用者	2010
12	PIN	7179				管理部	マネージャー	スキャナレベル		使用者	2010
13	PIN	777						スキャナレベル		使用者	2010
14	PIN	8787					顧問	スキャナレベル		使用者	2010
15	PIN	987				技術部	マネージャー	スキャナレベル		管理者	2010

5.4.1 認証

使用者を選択し、[認証]ボタンをクリックして、認証に用いる VP-II X ユニットを選択します。選択した PIN またはカード番号がその VP-II X ユニットに送信されます。使用者は、PIN の入力またはカードの提示を行わずに、手を入力するだけで認証することができます。

5.4.2 使用者の削除／管理者の削除

使用者のリストから使用者を1人または複数選択して、[使用者の削除]ボタンをクリックします。選択した使用者がデータベースから削除されます。この機能を使用するには、マスタユニットが動作していなければなりません。

管理者の削除: 管理者は削除機能では削除できません。管理者を削除するには、まず、後述の[使用者の変更]機能を使用して、使用者のタイプを管理者から使用者に変更する必要があります。

5.5 使用者の変更

メニュー:[使用者] > [使用者管理] > [使用者の変更]

使用者情報を入力または変更するには、リストから目的の使用者をダブルクリックするか、1 人または複数の使用者を選択してから[使用者の変更]ボタンをクリックします。下のウィンドウは、使用者を 1 人選択したときに表示されます。複数の使用者を選択した場合、複数の使用者に重複して設定できる項目だけが表示されます。

使用者情報はすべて、VP-II X 機器の情報と同期する必要があるため、このメニューから項目を変更する場合は、マスタユニットが動作していなければなりません。

5.5.1 使用者情報／パスワード

[PIN]と[登録日時]を除き、このウィンドウに表示されている項目はどれでも入力または変更可能です。適切に設定し、[変更]をクリックして適用します。各項目の説明については、前述の「第 2 章 5.3 使用者の登録」を参照してください。

[パスワード]オプションは、使用者にパスワードが割り当てられている場合のみ使用できます。この機能を使用するには、まず、パスワードを割り当てます。パスワードの割り当てまたは削除には、[パスワード]タブを使用します。個々の使用者に割り当てられたパスワードは表示できないため、パスワードを忘れてしまった場合は、新たに割り当てる必要があります。

5.5.2 カスタム定義

[カスタム定義]の内容は、あらかじめ定義されている場合のみ、入力または変更できます。カスタム定義可能なフィールドの使用法については、「第 2 章 5.2 使用者のカスタム定義」を参照してください。

5.5.3 静脈データ登録／再登録

事前登録使用者のために静脈データを登録したり、登録済み使用者の静脈データを更新(再登録)したりすることができます。

事前登録使用者は、[事前登録]機能を使って、PIN、氏名、社員 ID などの情報をすでに登録しているか、Excel ファイルからインポートしているが静脈データをまだ登録していない使用者です。

下のメニューは登録済み静脈データのステータスを示しています。[1]または[2](静脈データ番号)を選択するか、どちらも選択せずに、[静脈データ登録/再登録]ボタンをクリックして、静脈データを登録または再登録します。登録に使用する VP-II X ユニットの割り当てが必要です。

左手または右手に 1 つまたは 2 つのデータ、もしくは右手と左手に 1 つずつのデータを登録するか、何も登録しないことができます。「左手」、「右手」、「なし」など、各データの説明を入力できます。

使用者[PIN: 3291]

登録機:
エントランス [192.168.21.234]

静脈データ登録状態:

	情報	ステータス	最終更新日時
1	右手	登録済み	2010/08/26 8:27:11
2	左手		

静脈データ登録/再登録 削除

変更 キャンセル

5.6 使用者のインポート/エクスポート/事前登録

メニュー:[使用者] > [使用者管理] > [インポート/エクスポート]

5.6.1 使用者情報のエクスポート

使用者管理ウィンドウの使用者リストで、エクスポートする使用者を選択し、[インポート/エクスポート]ボタンをクリックします。下のウィンドウが表示されたら、[名前を付けて保存]を実行します。表示されたデータが Microsoft Excel 形式のファイルに保存されます。エクスポートされた Excel ファイルのシートは NetControl-X により保護されているため、このファイルを編集するには、シートの保護を解除する必要があります。

インポート/エクスポート

PINタイプ	PIN	名	姓	社員ID	所属	職位	使用者グループ
[00]PIN	[007]						
[00]PIN	[0221]						
[00]PIN	[11]						
[00]PIN	[13]				営業部	マネージャー	
[00]PIN	[16]						
[03]カード	[1793306731]						
[00]PIN	[3291]						
[03]カード	[3395269034]						
[00]PIN	[4570]						
[00]PIN	[67]				技術部		
[00]PIN	[71]				ゲスト		
[00]PIN	[7179]				管理部	マネージャー	
[00]PIN	[8787]						
[00]PIN	[987]				技術部	マネージャー	

データベースに存在しないPINを自動的に作成する
 システムに適用する場合、形式や内容が間違っている項目はデフォルト値を使用します

ファイルを開く 保存 事前登録 クリア 適用 閉じる

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
1	PINタイプ	PIN	名	姓	社員ID	所属	職位	使用者グループ	セキュリティ	使用者タイプ	有効期間	有効期限	有効無効	通行許可グループ	ビット長	サイトコード	ビット長	サイトコード
2	[00]PIN	[007]							[2]	[1]管理者			[1]無効					
3	[00]PIN	[0221]							[0]VIP-II X	[0]使用者			[1]無効					
4	[00]PIN	[11]							[0]VIP-II X	[0]使用者			[1]無効					
5	[00]PIN	[13]				営業部	マネージャー		[0]VIP-II X	[0]使用者			[1]無効					
6	[00]PIN	[16]							[0]VIP-II X	[0]使用者			[1]無効					
7																		
8																		

5.6.2 使用者情報のインポート

別のアプリケーションから使用者をインポートするには、Microsoft Excel ファイルをインポートします。使用者をインポートするには、[ファイルを開く]をクリックします。

データフィールドやフォーマットは指定された要件 (NetControl-X でエクスポートされたファイルと同じ) を満たしていなければなりません。Excel ファイルに必須のフィールドとデータフォーマットは次のとおりです。

□ オプション

オプション 1 [データベースに存在しない ID のため使用者のデータを自動的に作成する]

このオプションが選択されているとき、NetControl-X データベースに PIN やカード番号が存在しない (登録済み使用者ではない) 場合、NetControl-X はこれらの使用者を静脈データで事前登録します。静脈データは、[静脈データ再登録]機能を使用して別途登録する必要があります。静脈データの登録方法については、「第 2 章 5.5.3 静脈データ登録/再登録」を参照してください。

選択されていない場合、使用者はインポートされません。

オプション 2 [システムに適用する場合、形式や内容が間違っている項目はデフォルト値を使用します]

このオプションが選択されている場合、インポートされたファイルに誤った形式や内容が発見されると、デフォルト値が使用されます。選択されていない場合、誤った形式や内容があるデータは受け付けられません。

□ データフィールドとフォーマット

先頭行には項目名が入ることになっているため、インポートされません。ユーザーデータは 2 行目から入力します。セルの書式は「標準」または「文字列」に設定する必要があります。

[]で示されているフィールドには、「PIN 使用者」に対して[00]のように、半角の角かっこで囲んでデータを入力する必要があります。データ長については、下の説明を参照してください。

列 A、B、および J には必ず入力してください。列 A または J にデータが入っていない、または誤ったデータが入力されている場合、前述のオプション 2 が選択されていればデフォルト値が自動的に使用され(デフォルト: ID タイプ=[00]、使用者タイプ=[0])、オプションが選択されていなければ使用者はインポートされません。ID(列 B)が見つからない使用者は、どちらの場合でもインポートされません。

ID タイプが[01](カード使用者)の場合は、列 O、P、および Q も必須です。必須ではないフィールドは空白にすることができます。

	A	B	C	D	E	F	G	H
1	PIN タイプ	PIN	名	姓	社員 ID	所属	職位	使用者グループ
2	[]	[]						
	ID またはカード [00] ID [01] カード	[ID] [カード 番号]	それぞれ 50 文字まで					

	I	J	K	L	M
1	セキュリティレベル	使用者タイプ	有効時間	有効期限	有効/無効
2	[]	[]	[]	[]	[]
	[0] VP-II X のレベルを使用 [1]~[5] 個人別レベル	[0] 使用者 [1] 管理者	[yyyy-mm-dd hh:mm]		[1] 有効 [0] 無効

	N	O	P	Q
1	通行許可グループ	総ビット長	サイトコードビット長	サイトコード
2	[]			
	テーブル番号(3桁) [001] ~ [200]	Wiegand ビット長 26 ~ 128	0~126	サイトコードの値

□ 例

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	PIN タイプ	PIN	名	姓	社員ID	所属	職位	使用者グループ	セキュリティレベル	使用者タイプ	有効時間	有効期限	有効/無効	通行許可グループ	総ビット長	サイトコードビット長	サイトコード
2	[00]PIN	[007]							[2]	[1]管理者		[2010-08-20 13:05]	[1]無効	[001]			
3	[00]PIN	[0221]						[0]VP-II X	[0]使用者				[1]有効		26	8	100
4																	

5.6.3 事前登録

メニュー:[使用者] > [使用者管理] > [インポート/エクスポート] > [事前登録]

事前登録では、使用者情報の PIN やカード番号をあらかじめ入力またはインポートしておいた使用者の登録を行うことができます。このメニューから登録した使用者は、[静脈データ再登録]を使用して静脈データを登録する必要があります。静脈データの登録方法については、「第 2 章 5.5.3 静脈データ登録/再登録」を参照してください。

□ 認証方法

登録する PIN タイプを、(PIN、Prox カード)から選択します。

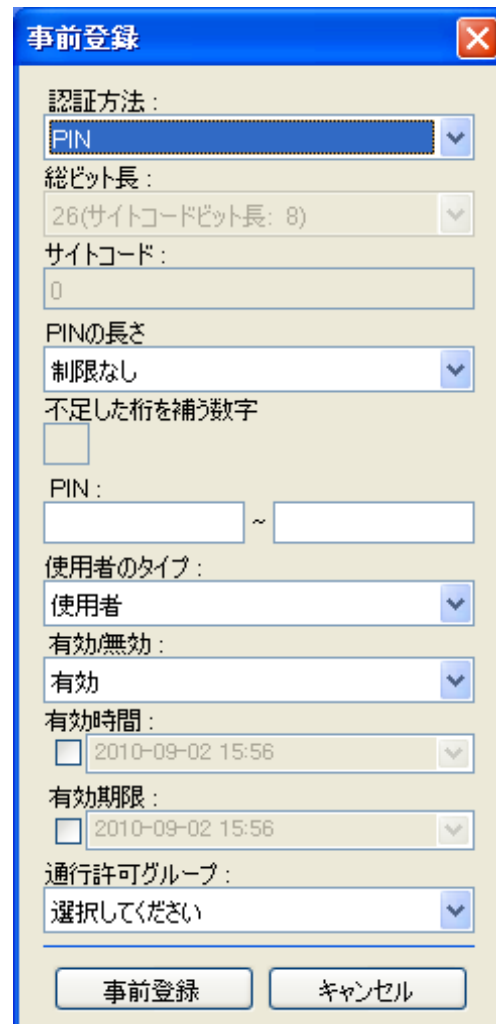
□ 総ビット長/サイトコード

カード番号を登録する場合、Wiegand ビット長を選択し、サイトコードを入力します。[設定] > [Wiegand フォーマット設定]を使用して定義した Wiegand フォーマットについてのみ、サイトコードを入力できます。定義されていない Wiegand フォーマットを選択した場合、このサイトコードは使用されず、パリティビット以外のすべてのビットがカード番号に使用されます。

□ PIN の長さ

PIN を登録する場合、[PIN の長さ]と[不足した桁を補う数字]を設定することができます。たとえば、[PIN の長さ]に「5」、[不足した桁を補う数字]に「0」を設定した場合、[PIN]に「123」と入力すると、PIN は「00123」になります。

また、[使用者タイプ]、[有効時間]、[有効期限]、[通行許可グループ]も設定できます。



事前登録

認証方法：
PIN

総ビット長：
26(サイトコードビット長: 8)

サイトコード：
0

PINの長さ
制限なし

不足した桁を補う数字

PIN:
 ~

使用者のタイプ：
使用者

有効/無効：
有効

有効時間：
 2010-09-02 15:56

有効期限：
 2010-09-02 15:56

通行許可グループ：
選択してください

事前登録 キャンセル

5.7 削除予定の使用者リスト

メニュー:[使用者] > [削除予定の使用者リスト]

これは、検索結果に基づいて、特定の期間利用していない使用者を簡単に削除するための機能です。



	PIN	使用者タイプ	名前	所属	職位	最新のアクセス時間
1	3291	使用者				
2	4570	使用者				

期間: 最新 1 年 | 2009-08-20 ~ 2010-08-20

検索済み: 2

チェック | 削除 | 閉じる

[最新 1 年]、[最新 6 ヶ月]、[最新 3 ヶ月]の検索オプションが用意されています。また検索期間を指定する[カスタム]も選択できます。検索後、検索された使用者を削除することができます。削除した後、削除された使用者のリストを Excel ファイルとして保存することもできます。

5.8 再登録使用者リスト

メニュー:[使用者] > [再登録使用者リスト]

再登録使用者リスト

	PIN	使用者タイプ	名前	所属	職位	情報
1	007	管理者				連続して3回以上の認証失敗
2	16	使用者				連続して3回以上の認証失敗
3	1793306731	管理者				連続して3回以上の認証失敗
4	3395269034	使用者				連続して3回以上の認証失敗
5	67	管理者		技術部		連続して3回以上の認証失敗
6	8787	使用者				連続して3回以上の認証失敗
7	987	管理者		技術部	マネージャー	連続して3回以上の認証失敗

期間 2010-07-20 ~ 2010-08-20

チェックした状態 連続して3回以上の認証失敗

全て: 14 14

チェック 保存 閉じる

ある条件下で認証に失敗した使用者を検索することにより、認証に問題のある使用者を確認し、より確実に認証できるように再登録するかどうか判断することができます。また、管理の目的で、使用者リストを Excel ファイルとして保存することもできます。

6. レポート、イベント表示、データベースバックアップ/管理

6.1 レポート

使用者の入退室イベント、勤怠記録、システムログを Microsoft Excel ファイルにエクスポートし、レポート生成に使用できます。

6.1.1 レポートの共通オプション

□ 機能キーの選択

機能キーオプション

機能キーを使用したイベントのみを作成

全てのイベントのレポートを作成(機能キーの有無に関わらず)

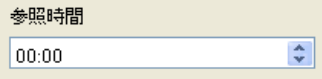
これは勤怠日報のためのオプションです。

システムを勤怠管理のために使用する場合、VP-II X の機能キー (F1/F2) は通常、勤怠記録のために PIN またはカードと組み合わせて使用されます。F1 は出勤 (入室)、F2 は退勤 (退室) に割り当てられています。この場合、使用者は機能キーを入力してから、PIN を入力するか、カードを提示します。機能キー情報 (F1 または F2) が入力された場合、このキー情報は使用者トランザクションのイベントデータに含まれます。

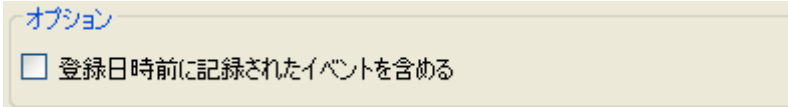
[機能キーを使用したイベントのみを作成] を選択した場合、機能キー F1 または F2 に関連付けられたイベントだけが、勤怠日報の作成や、ある 1 日の勤務時間 (出勤から退社までの時間) の計算に使用されます。選択した日に機能キーと関連付けられたイベントが存在しない場合、レポートは空白のまま、その日の勤務時間は計算されません。

[全てのイベントのレポートを作成 (機能キーの有無に関わらず)] を選択した場合、レポートには、機能キーの記録に関係なく、その日の最初のイベントが出勤として、最後のイベントが退勤として記録されます。上の例では、使用者が出勤時に誤って F1 キーを押し忘れたが、実際に認証された場合、データベースには認証成功イベントが記録され、レポートに使用されます。

□ 参照時間

 これは 1 日の始まりと見なされる時間で、通常午前 0 時です。たとえば、使用者が午後 10 時から翌日の午前 6 時まで勤務する場合、これを「22:00」(午後 10 時) に設定することができます。この使用者の記録は「前日の午後 10 時に出勤」し、「選択した日の午前 6 時に退勤」となります。また、その日の勤務時間は前日の午後 10 時から選択した日の午前 5 時 59 分までで計算されます。

□ 登録日時前に記録されたイベントを含める

 オプション
 登録日時前に記録されたイベントを含める

上のオプションは、登録日より前に記録されたイベントをレポートに入れるかどうかを指定します。

ある使用者が何らかの理由で削除され、指定された期間内に再び登録された場合、このオプションを選択すると、登録日より前に記録されたイベントも選択した使用者のイベントであるとみなされます (NetControl-X は、最後に登録した日付のみ保持しています)。

以前の使用者が使用していた PIN またはカードで別の使用者を新たに登録した場合には、このオプションの選択を解除すると、登録日以前に記録されたイベントは以前の使用者のものとなり、現在の使用者のレポートには含まれません。

□ プレビュー／印刷／保存

[プレビュー] をクリックすると、下の例にあるように、選択したレポートのレポートウィンドウが開きます。[保存] をクリックすると、データが Microsoft Excel ファイルにエクスポートされます。また、[印刷] をクリックするとプレビュー表示後に、印刷することができます。

プレビュー：勤怠 日報

	所属	PIN	名前	F1	F2	情報
1		007		17:22	18:31	
2		0221		17:22	18:05	
3		11		----	----	
4	営業部	13		18:15	18:15	
5		16		----	----	
6		1793306731		14:24	16:00	
7		3291		16:20	16:21	
8		3395269034		----	----	
9		4570		----	----	

印刷 保存 閉じる

□ エクスポートされたファイルの例

A12 fx

	A	B	C	D	E	
1	所属	PIN	名前	F1	F2	情報
2		007		17:22	18:31	
3		0221		17:22	18:05	
4		11		----	----	
5	営業部	13		18:15	18:15	
6		16		----	----	
7		1793306731		14:24	16:00	
8		3291		16:20	16:21	
9						
10						

6.1.2 勤怠日報

選択された日付について、すべての使用者の勤怠日報を選択し、生成することができます。前述のセクションで説明したとおり、機能キーオプションを選択し、参照時間を設定します。上の例を参照してください。

6.1.3 勤怠日報 使用者毎

選択した使用者について、選択した期間のレポートを生成することができます。検索条件を入力して目的の使用者を検索します。すべての使用者をリストするには[全ての使用者]をクリックします。次に、リストから使用者を選択し、目的の期間とオプションを設定します。「使用者」とは、現在データベースに登録されている使用者を意味します。完全な履歴レポートを作成するために、削除した使用者のレポートを作成することもできます。

レポート

- レポート種類
- 勤怠日報
- 勤怠 使用者毎
- 入退室レポート
- 機器イベントログ
- コマンドログ

勤怠 使用者毎

PIN 使用者

	PINタイプ	PIN	名前	社
1	PIN	007		
2	PIN	0221		
3	PIN	11		
4	PIN	13		営業部
5	PIN	16		
6	カード	1793308731		
7	PIN	3291		
8	カード	3395269034		
9	PIN	4570		

期間

開始時間

終了時間

参照時間

オプション

登録日時前に記録されたイベントを含める

機能キーオプション

機能キーを使用したイベントのみを作成

全てのイベントのレポートを作成(機能キーの有無に関わらず)

検索 詳細検索 全ての使用者

全てを選択 選択解除

プレビュー 閉じる

6.1.4 入退室レポート

使用者(PIN または名前)、機器、またはグループごとに、選択した期間の入退室記録すべてについてのレポートを生成することができます。認証タイプ(認証成功または認証失敗)を選択し、必要な期間を設定してから、PIN、名前、グループ、機器などを入力または選択します。このレポートには、脅迫認証、バイパス、認証方法(手の甲かパスワードか)、認証成功までの試行回数、静脈データ番号など、入退室に使用された情報がすべて表示されます。

プレビュー：入退室レポート

	時間	認証タイプ	機器	PINタイプ	PIN	名前	使用者タイプ	機能キー	使用者の認証方法	認
1	2010-08-20 07:51:07	使用者認証	エントランス	PIN	7179		使用者	未使用	PIN	PI
2	2010-08-20 08:07:37	使用者認証	エントランス	PIN	7179		使用者	未使用	PIN	PI
3	2010-08-20 08:19:35	使用者認証	エントランス	PIN	7179		使用者	未使用	PIN	PI
4	2010-08-20 08:25:43	使用者認証	エントランス	PIN	67		管理者	未使用	PIN	PI
5	2010-08-20 08:26:28	使用者認証	エントランス	PIN	67		管理者	未使用	PIN	PI
6	2010-08-20 08:31:31	使用者認証	エントランス	PIN	7179		使用者	未使用	PIN	PI
7	2010-08-20 08:37:07	使用者認証	エントランス	PIN	7179		使用者	未使用	PIN	PI
8	2010-08-20 08:41:07	使用者認証	エントランス	PIN	7179		使用者	未使用	PIN	PI
9	2010-08-20 08:42:10	使用者認証	エントランス	PIN	007		管理者	未使用	PIN	PI
10	2010-08-20 08:43:57	使用者認証	エントランス	PIN	16		使用者	未使用	PIN	PI
11	2010-08-20 09:15:59	使用者認証	エントランス	PIN	13		使用者	未使用	PIN	PI
12	2010-08-20 09:29:40	使用者認証	エントランス	PIN	67		管理者	未使用	PIN	PI
13	2010-08-20 09:30:53	使用者認証	エントランス	PIN	67		管理者	未使用	PIN	PI

保存 閉じる

6.1.5 機器ログ／イベント

選択した期間について、機器単位、機器グループ単位、またはすべての機器について、機器レポートを生成できます。

機器レポートに含めることのできるイベントは、使用者の登録と削除、VP-II X の管理者メニューで変更された使用者情報、VP-II X の設定変更、機器履歴、扉履歴です。目的の機器または機器グループとイベント種類を選択してください。

プレビュー：機器イベント/ログ

時間	イベント種類	機器	使用者	使用者 タイプ	説明
13	2010-08-20 08:26:30	扉履歴	エントランス		認証による解錠
14	2010-08-20 08:26:37	扉履歴	エントランス		認証による扉開閉
15	2010-08-20 08:28:51	扉履歴	エントランス		解錠ボタンによる解錠
16	2010-08-20 08:28:59	扉履歴	エントランス		解錠ボタンによる扉開閉
17	2010-08-20 08:31:33	扉履歴	エントランス		認証による解錠
18	2010-08-20 08:31:40	扉履歴	エントランス		認証による扉開閉
19	2010-08-20 08:32:41	扉履歴	エントランス		解錠ボタンによる解錠
20	2010-08-20 08:32:48	扉履歴	エントランス		解錠ボタンによる扉開閉
21	2010-08-20 08:37:07	扉履歴	エントランス		認証による解錠
22	2010-08-20 08:37:14	扉履歴	エントランス		認証による扉開閉
23	2010-08-20 08:40:42	扉履歴	エントランス		解錠ボタンによる解錠
24	2010-08-20 08:40:48	扉履歴	エントランス		解錠ボタンによる扉開閉
25	2010-08-20 08:41:08	扉履歴	エントランス		認証による解錠
26	2010-08-20 08:41:15	扉履歴	エントランス		認証による扉開閉
27	2010-08-20 08:42:11	扉履歴	エントランス		認証による解錠
28	2010-08-20 08:42:18	扉履歴	エントランス		認証による扉開閉

保存 閉じる

6.1.6 コマンドログ

NetControl-X で実行されたコマンドログをすべて表示したレポートを生成します。これは、トラブルシューティングですべての NetControl-X 操作の履歴が必要とされた場合に便利です。一般の使用者には、この機能の使用はお勧めしません。

6.1.7 勤怠日報(TNA)

選択された日付について、すべての使用者の勤怠日報を選択し、生成、自動的に稼働時間を計算表示することができます。また F3(外出)、F4(戻り)使用時の[外出可能回数、[切り捨て時間の基準]を設定することができます。

6.1.8 勤怠日報 使用者毎(TNA)

選択した使用者について、選択した期間のレポートを生成することができます。検索条件を入力して目的の使用者を検索します。すべての使用者をリストするには[全ての使用者]をクリックします。次に、リストから使用者を選択し、目的の期間とオプションを設定します。「使用者」とは、現在データベースに登録されている使用者を意味します。完全な履歴レポートを作成するために、削除した使用者のレポートを作成することもできます。また F3(外出)、F4(戻り)使用時の[外出可能回数、[切り捨て時間の基準]を設定することができます。

6.2 イベント表示

イベント表示には、データベースに登録されているすべてのログ(使用者、システムイベント、コマンド)が表示されます。この機能は、システム管理者のために、すべてのシステム履歴および使用者トランザクション履歴を提供します。

6.3 データベースバックアップ/整理

データベース、削除済みイベント、およびタスクコマンドすべてのバックアップと管理を行います。ファイルは CSV 形式で保存されます。

データベースバックアップ/整理

バックアップ

データベースと履歴のバックアップ
バックアップファイルは データベースのバックアップフォルダに保存されます。

実行

イベント整理

整理したイベントデータはバックアップファイルに保存されます。保存されたデータは元のデータベースから削除されます。

2010-08-23 16:48 ~ 2010-08-23 16:48

実行

コマンド整理

整理したコマンド(タスク)データはバックアップファイルに保存されます。保存されたデータは元のデータベースから削除されます。

2010-08-23 16:48 ~ 2010-08-23 16:48

実行

閉じる

6.3.1 バックアップ

データベースと履歴はサーバに保存されます。バックアップファイルには拡張子「.bak」または「.log」がつけられ、SQL Server のバックアップフォルダ

「C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup」に保存されます。

6.3.2 イベント整理

これは、データベースからのシステムイベントの整理に使用されます。このコマンドを実行すると、NetControl-X は、すべての情報とシステムイベントを CSV ファイルとして保存し、その後、データベースから削除します。

6.3.3 コマンド整理

これは、XAgent からデータベース経由で送受信されるコマンドタスクに関連するコマンドや応答を整理するために使用されます。このコマンドを実行すると、NetControl-X は、これらの情報を CSV ファイルとして保存し、その後、データベースから削除します。

第 3 章 付録

1. インストール

1.1 NetControl-X をインストールするためのシステム要件

	項目	基本仕様	推奨される仕様
XAgent	CPU	Pentium 4 - 2.4GHz 以上	Pentium 4 - 3GHz 以上
	RAM	512 MB	1 GB
	OS	Windows XP Professional 以上 Windows Server 2000	Windows XP Professional 以上 Windows Server 2003 Windows Vista Business Windows 7 Professional Windows Server 2008R2
DBMS	CPU	Pentium 4 - 2.4GHz 以上	Pentium 4 Xeon (DualCPU) 3GHz 以上
	RAM	512 MB	2 GB
	OS	Windows XP Professional 以上 Windows Server 2003	Windows XP Professional 以上 Windows Server 2003 Windows Vista Business Windows 7 Professional Windows Server 2008R2
NetControl-X	CPU	Pentium III – 600MHz	Pentium 4 - 2GHz
	RAM	256Mbyte	512Mbyte
	OS	Windows XP Professional 以上	Windows XP Professional 以上 Windows Server 2003 Standard Windows Vista Business Windows 7 Professional Windows Server 2008R2 Standard
XConfig	CPU	Pentium III – 600MHz	Pentium 4 - 2GHz
	RAM	256Mbyte	512Mbyte
	OS	Windows XP Professional 以上	Windows XP Professional 以上 Windows Server 2003 Standard Windows Vista Business Windows 7 Professional Windows Server 2008R2 Standard

1.2 インストール

インストールプログラムは、インストール CD を挿入すると自動的に起動されます。または、インストール CD から AUTORUN.EXE を実行します。次のインストールウィンドウが表示されます。[ALL SETUP]またはインストールするコンポーネントを選択し、[INSTALL]をクリックして開始します。インストール CD で各コンポーネントのディレクトリにある「setup.exe」ファイルを実行して、コンポーネントを個別にインストールすることもできます。



最初に、プログラムのインストールに使用する言語を選択する必要があります。言語を選択し、インストールプログラムの指示に従って操作します。詳細は、以下のセクションを参照してください。

NetControl-X コンポーネントがインストールされるデフォルトディレクトリは次のとおりです。

C:\Program Files\HVPR\NetControl-X

C:\Program Files\HVPR\HVPR-X DB

C:\Program Files\HVPR\XAgent

C:\Program Files\HVPR\XConfig

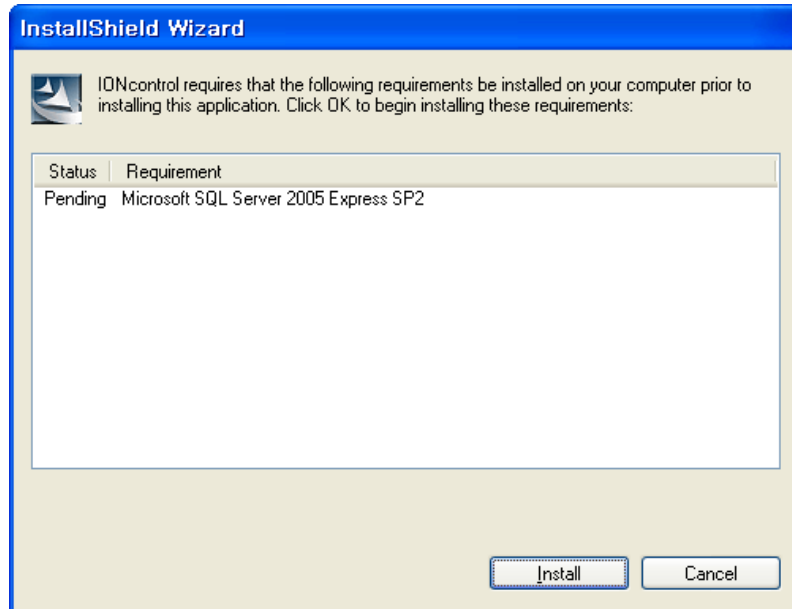
HVPR は、Hand Vascular Pattern Recognition system (手の甲静脈認証システム) の略です。

1.3 DBMS (MS-SQL) のインストール

NetControl-X では、データベースとして MS-SQL が使用されます。インストールするコンピュータで SQL Server が見つからない場合、NetControl-X のインストーラにより、Microsoft SQL Server 2005 Express がインストールされます。

1.3.1 Microsoft SQL Server 2005 Express のインストール

Microsoft SQL Server が見つからない場合、次のウィンドウが表示されます。[Install] ボタンをクリックして、次のステップに進み、Microsoft SQL Server 2005 Express をインストールします。



最初に、Windows Installer 3.1 や Microsoft .Net Framework 2.0 など、Microsoft SQL Server 2005 Express のインストールに必要なコンポーネントがインストールされます。次に、Microsoft SQL Server 2005 Express が自動的にインストールされます。これには数分間かかります。インストールが完了するまで待ちます。Microsoft SQL Server 2005 Express のインストールが正常に終了すると、次のセクションに示す NetControl-X データベースをインストールするためのウィンドウが表示されます。

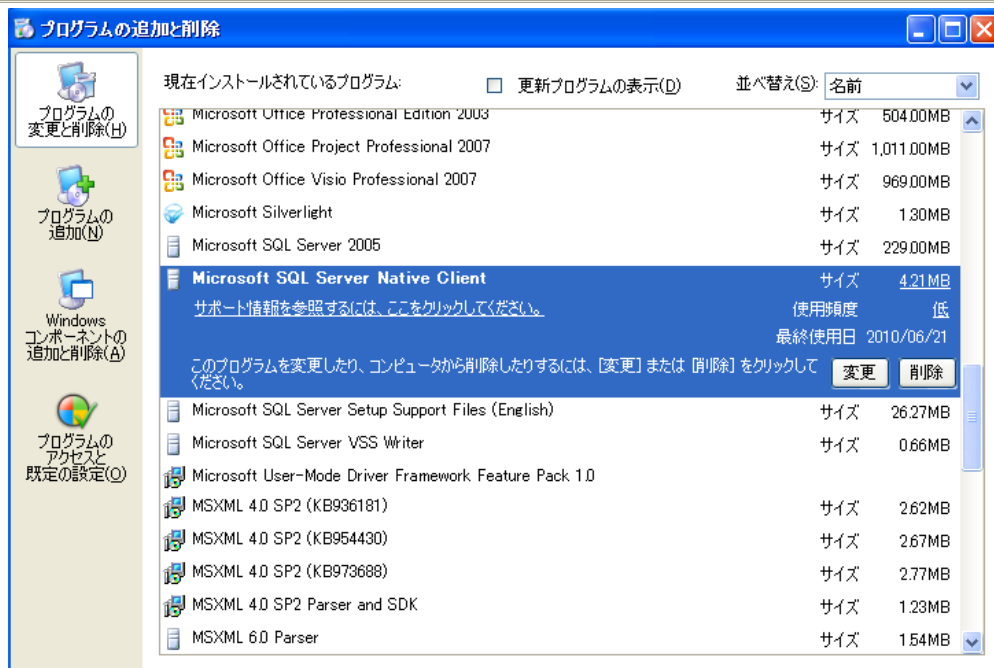
トラブルシューティング



インストール中、上のエラーが発生した場合は、[No] ボタンをクリックしてインストールを中止し、以下の点を確認してください。

❑ Microsoft SQL Server Native Client

Microsoft SQL Server Native Client が正しくインストールされていない場合、前述のエラーが発生することがあります。コントロールパネルの[プログラムの追加と削除]を使用して Microsoft SQL Server Native Client を削除してから、DBMS を再インストールしてください。



□ システム要件

Microsoft SQL Server Native Client を再インストールしてもこのエラーが消えない場合は、Microsoft SQL Server 2005 Express のインストールにおける以下の最小システム要件を満たしているかどうかを確認します。

O/S: Windows 2000 SP5、Windows Server 2003 SP1、Windows Vista、Windows XP SP2

最小ハードディスク空き容量: 2.0GByte

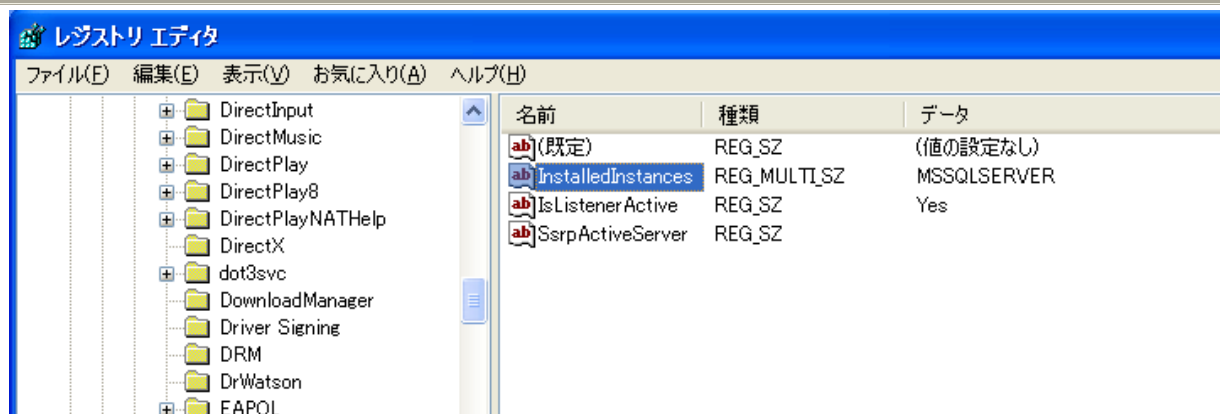
必須インストール項目: Internet Explorer 6.0 SP1 以上、Windows Installer 3.1 以上、Microsoft Data Access Components (MDAC) 2.8 SP1、Microsoft .NET Framework 2.0

1.3.2 既存の Microsoft SQL Server の使用

Microsoft SQL Server が見つかったと、NetControl-X インストーラは前述の手順をスキップして、NetControl-X データベースをインストールするための手順に進みます。以下のセクションを参照してください。

トラブルシューティング

使用しているコンピュータにすでに Microsoft SQL Server がインストールされているにもかかわらず NetControl インストーラが Microsoft SQL Server 2005 Express をインストールしようとする場合、インストールを終了し、下の図に示すシステムレジストリの値を確認してください。NetControl インストーラはレジストリの値を確認し、システムレジストリに下の図のようなデータまたは値がない場合は、Microsoft SQL Server は存在しないと判断します。



1.3.3 NetControl-X データベースのインストール

MS-SQL Express 2005 Server のインストールが完了すると、引き続き、NetControl-X Database のインストールが行われます。これにより、NetControl-X で使用される SQLDBMS データベースのアカウントとテーブルが作成されます。[次へ]をクリックして続行します。



まず、下の図に示すように、データベースサーバと認証方法の選択が求められます。



既存の Microsoft SQL サーバを使用する場合は、SQL データベースがインストールされている場所の IP アドレスを入力するか、[参照]からサーバを選択します。

NetControl から SQL サーバにアクセスできるように、管理者のログイン ID とパスワードを入力します。NetControl によりインストールされた Microsoft SQL 2005 Express を使用している場合は、[次へ]ボタンをクリックして続行します。ログイン ID「sa」は、NetControl インストーラによりデフォルトで作成される管理者用アカウントです。デフォルトのパスワードは「sql2005」です。後でこのパスワードを変更することもできます。

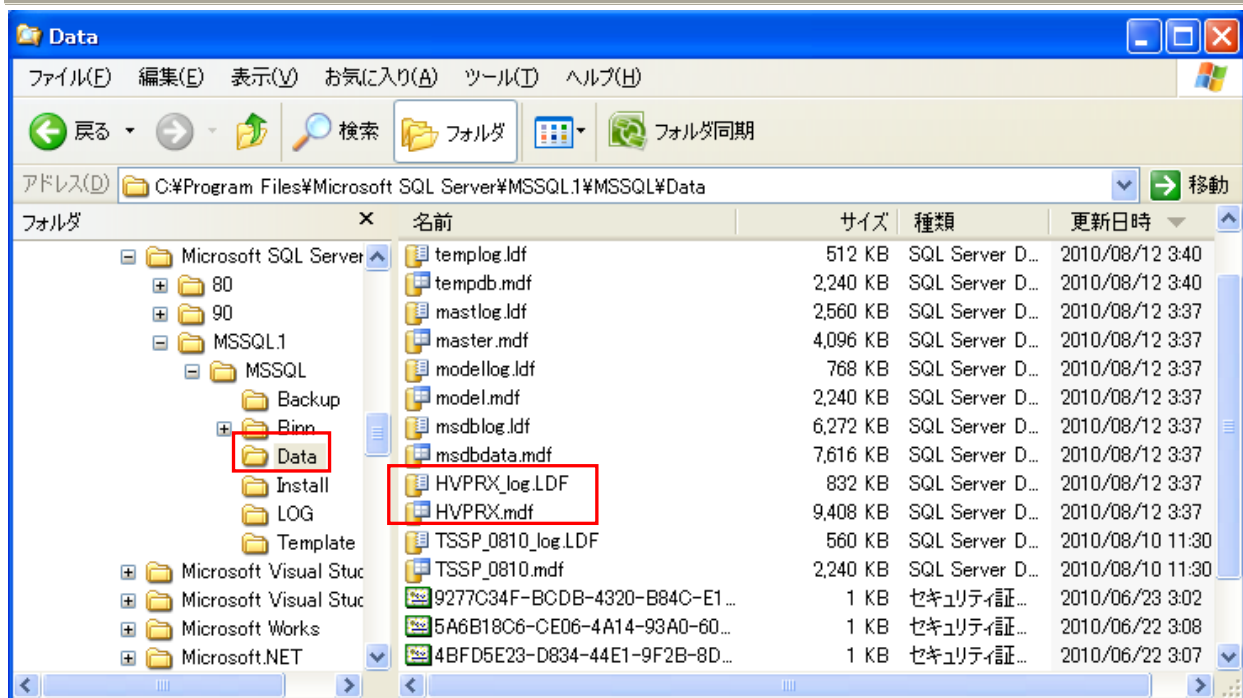
データベースがインストール先と同じコンピュータ(127.0.0.1)にインストールされている場合、Windows 管理者のアカウントでログインしていれば、[現在のユーザーの Windows 認証資格情報]を使用することもできます。管理者としてログインしていない場合、システムへのアクセス権が一部制限されます。

トラブルシューティング:DBMSの再インストール

既存の NetControl-X データベースを削除した後で再インストールする場合、次のエラーが発生することがあります。

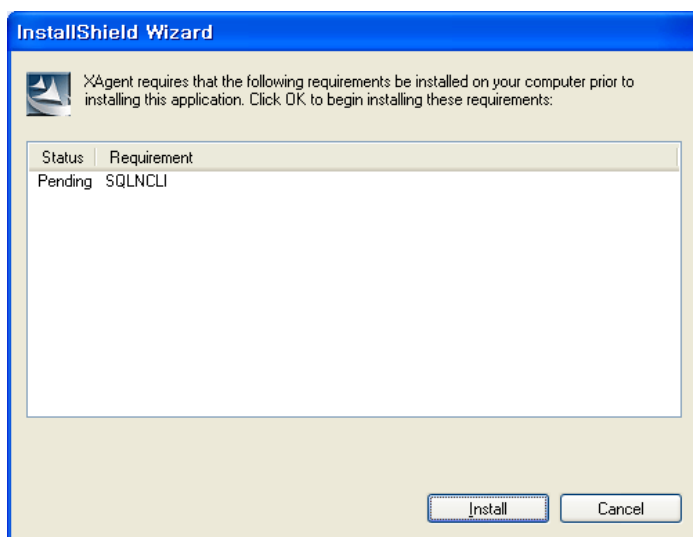


上のエラーが発生した場合、下の図にあるように、SQL Server がインストールされている data フォルダから HVPRX.mdf ファイルと HVPR_log.ldf ファイルを削除する必要があります。

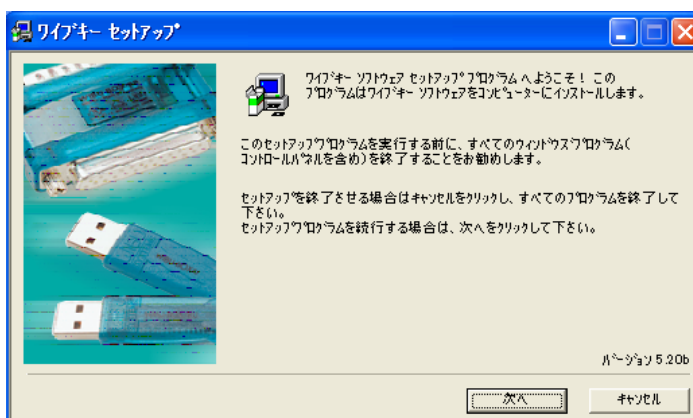


1.4 XAgent／ワイブキーのインストール

XAgent プログラムを使用するコンピュータには、SQLNCLI コンポーネントがインストールされている必要があります。このコンポーネントが見つからない場合、XAgent のインストール前にインストールされます。



[インストール]をクリックし、下の図に示す手順が表示されるまで、画面の指示に従って操作します。ソフトウェア保護のため、XAgent は Wibu キーを必要とするため、Wibu キー用のドライバもインストールされます。



[次へ]ボタンをクリックして、ワイブキーのインストーラが示す手順に従って操作し、ワイブキーのインストールを完了します。[完了]ボタンをクリックして、XAgent のインストールを完了します。

XAgent のインストールが正常に終了したら、DBMS に接続するための初期設定が必要です。詳細は、「第 1 章 2.3 XAgent のセットアップ」を参照してください。XAgent は Windows サービスに登録され、PC を起動すると自動的に実行されます。

1.5 XConfig／NetControl-X のインストール

XConfig および NetControl-X のインストールは簡単です。インストールウィンドウに表示される手順に従って操作してください。

2. XConfig

XConfig は、VP-II X ユニットのネットワークパラメータのセットアップ、データベースへの VP-II X ユニットの登録、ファームウェアのアップグレード、データベースへの VP-II X のバックアップおよびリストアに使用されるソフトウェアツールです。

注意: XConfig では、TCP/IP ポート番号に 61200、UDP ポートに 61201/61202 が使用されます。他のアプリケーションが既にこれらのポートを使用している場合、XConfig は起動されません。

XConfig を実行するか、[Search (F5)]をクリックすると、XConfig はブロードキャスト範囲内でそのときにネットワークに接続されている VP-II X ユニットのすべてを表示します。

2.1 VP-II X ネットワークパラメータのセットアップ

下の図で赤い丸で示されているチェックボックスをオンにして、変更する VP-II X を選択します。[Check All (F1)] をオンにして、すべてのユニットを選択することもできます。次に、列をダブルクリックして編集するか、[DHCP]または[Master]/[Slave]を選択し、[Save (F6)]ボタンをクリックして適用します。[Save (F6)]を実行しなかった場合、変更は適用されません。

変更を保存するには、ネットワークパスワードを入力する必要があります。このパスワードはデフォルトで「admin」です。処理結果は[結果]列に表示されます。結果を確認します。正常に終了した場合は赤字で「O.K.」と表示されます。「Timeout」または「Failure」と表示される場合はやり直してください。

Master IP: マスタユニットの IP アドレス。

Server IP: XAgent が実行されているサーバの IP アドレス。

DHCP: このオプションがオンになっている場合、VP-II X は DHCP サーバから IP アドレスを取得します。マスタユニットでは、このオプションを使用せず常に同じ IP アドレスを使用する場合があります。DHCP が有効な場合、IP、サブネットマスク、ゲートウェイは変更できません。

Port: TCP/IP コミュニケーションポート。

H.B. (Master Interval): マスタユニットとスレーブユニットの間のハートビートプロトコルの間隔を設定します。スレーブユニットは定期的にマスタユニットにハートビートプロトコルを送信し、通信ステータスを確認します。

Master/Slave: マスタに設定されるユニットは 1 つのみです。その他はすべてスレーブになります。

Version: VP-II X に適用されるファームウェアプログラムには、Boot、Kernel、Ramdisk、Application、Media の 5 種類があります。この列には Application ファームウェアのバージョンのみ表示されます。その他は最下部に表示されます。

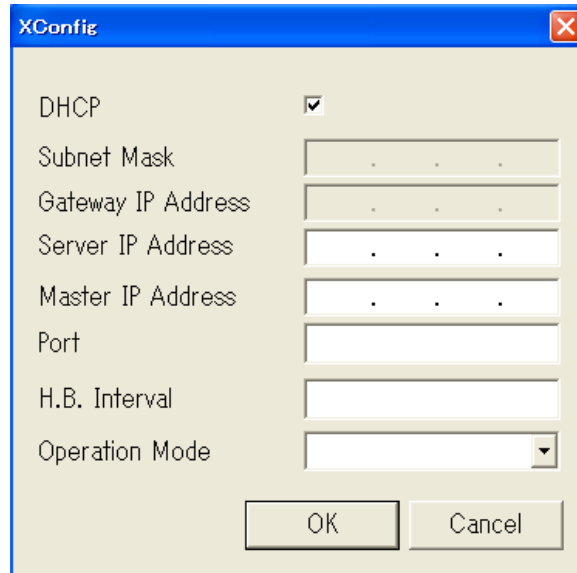
#	MAC	DHCP	IP	Subnet mask	Gateway	Server IP	Master IP	Port	H.B...	Master	Slave	Version	Result
1	00:15:10:70:16:03	<input type="checkbox"/>	192,168,21,249	255,255,255,0	192,168,21,254	192,168,21,82	192,168,21,234	61235	10	<input type="radio"/>	<input type="radio"/>	0,1,14:v163	
2	00:15:10:70:07:93	<input checked="" type="checkbox"/>	192,168,21,234	255,255,255,0	192,168,21,254	192,168,21,82	192,168,21,234	61235	10	<input type="radio"/>	<input type="radio"/>	0,1,14:v165	
3	00:15:10:70:25:51	<input checked="" type="checkbox"/>	192,168,21,85	255,255,255,0	192,168,21,254	0,0,0,0	128,0,0,1	61235	10	<input type="radio"/>	<input type="radio"/>	0,1,14:v133	
4	00:15:10:70:25:47	<input type="checkbox"/>	128,0,0,1	255,255,255,0	128,0,0,1	0,0,0,0	128,0,0,1	61235	10	<input type="radio"/>	<input type="radio"/>	0,1,14:v165	

[F/W Ver] [BOOT] :0,1,3:v2 [KERNEL] :0,1,4:v5 [RAMDISK] :0,1,1:v4 [APP] :0,1,14:v163 [MEDIA] :0,1,10:v1_voice_addon_en [Default password]

Search (F5) Save (F6) Download (F7) Batch (F8) Password (F9) Backup (F3) Restore (F4) Close (Esc)

□ Batch(F8)

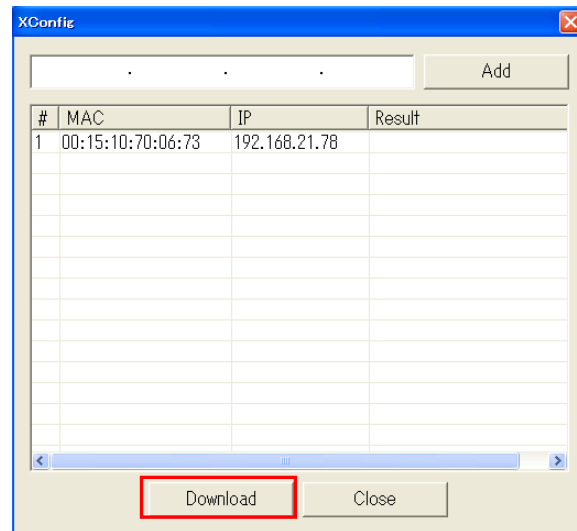
これは複数の VP-II X に対して一度に共通するパラメータを設定するための機能です。チェックボックスをクリックして目的のユニットを選択してから[Batch(F8)]ボタンをクリックすると、次のウィンドウが表示されます。パラメータを入力し、[OK]ボタンをクリックして適用します。変更しないフィールドは空白のままにしておいてかまいません。



DHCP	<input checked="" type="checkbox"/>
Subnet Mask	. . .
Gateway IP Address	. . .
Server IP Address	. . .
Master IP Address	. . .
Port	
H.B. Interval	
Operation Mode	

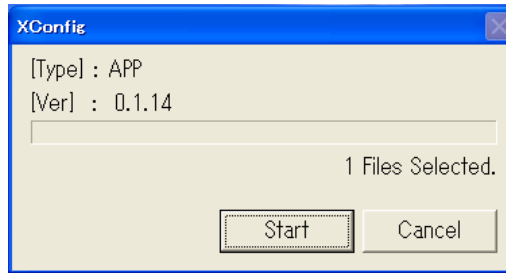
2.2 ファームウェアのダウンロード／アップグレード

ファームウェアをダウンロードする VP-II X を選択(左側のチェックボックスをクリック)し、[Download(F7)]をクリックしてファームウェアファイルをロードします。各 VP-II X の TCP/IP アドレスを入力し、「Add」をクリックすることによりリストに追加することもできます。



#	MAC	IP	Result
1	00:15:10:70:06:73	192.168.21.78	

Windows のファイル検索ウィンドウから、アップグレードするファームウェアファイルを選択し、[Start]ボタンをクリックしてダウンロードを開始します。



インストールの完了メッセージが表示されるまで待ちます。また、VP-II X にもダウンロードの進捗状況が表示されます。VP-II X は、フラッシュメモリにファームウェアを書き込むと、自動的に再起動します。メモリに完全にファームウェアを書き込むには、VP-II X の電源を入れたままにしておく必要があります。ファームウェアのアップグレード中に電源を切ると、ファームウェアのインストールが不完全になり、システムが動かなくなる可能性があります。

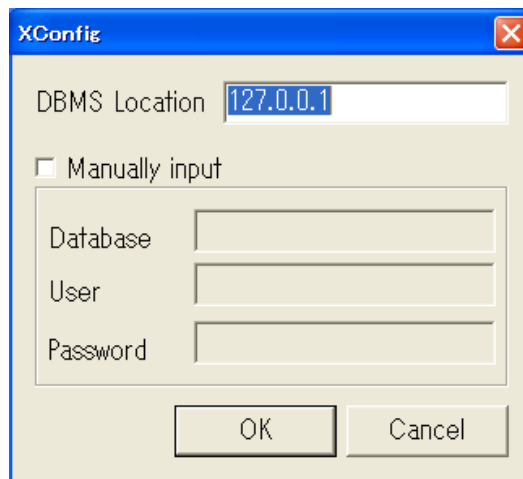
2.3 DBMS への VP-II X の登録 — DB へ追加(F2)

これは、VP-II X の情報を NetControl のデータベースに登録して、NetControl-X やその他の SDK を使用して実装されるアプリケーションで使用できるようにするための機能です。この手順は、NetControl-X を実行する前に必ず実行してください。

VP-II X ユニットのチェックボックスをオンにし、[Add to DB(F2)]ボタンをクリックします。

[DBMS Location]フィールドに、DBMS がインストールされているサーバの IP アドレスを入力し、[OK]をクリックして登録します。DBMS がローカルコンピュータにインストールされている場合、下の例に表示されているように「127.0.0.1」と入力してください。

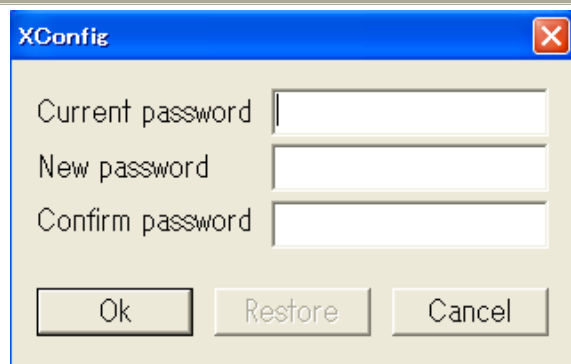
[手動で入力]オプションを選択した場合、データベース名、アカウント、パスワードを手動で入力できます。選択しない場合、NetControl-X のインストール時に作成されたデフォルトデータベースに接続されます。



2.4 パスワード／バックアップ／リストア

□ Password(F9)

パスワードは変更できます。このパスワードはデフォルトで「admin」です。このパスワードは NetControl-X コンポーネントと VP-II X の間の通信すべてに使用されます。また、前述のとおり、ネットワークパラメータのセットアップやファームウェアのダウンロードにもこのパスワードが必要になります。



□ Backup (F3) / Restore (F4)

VP-II Xにある現在の使用者データベース/VP-II Xのシステム設定情報をバックアップおよびリストアすることができます。

User[IP アドレス].dat ※使用者データベース(静脈データ)

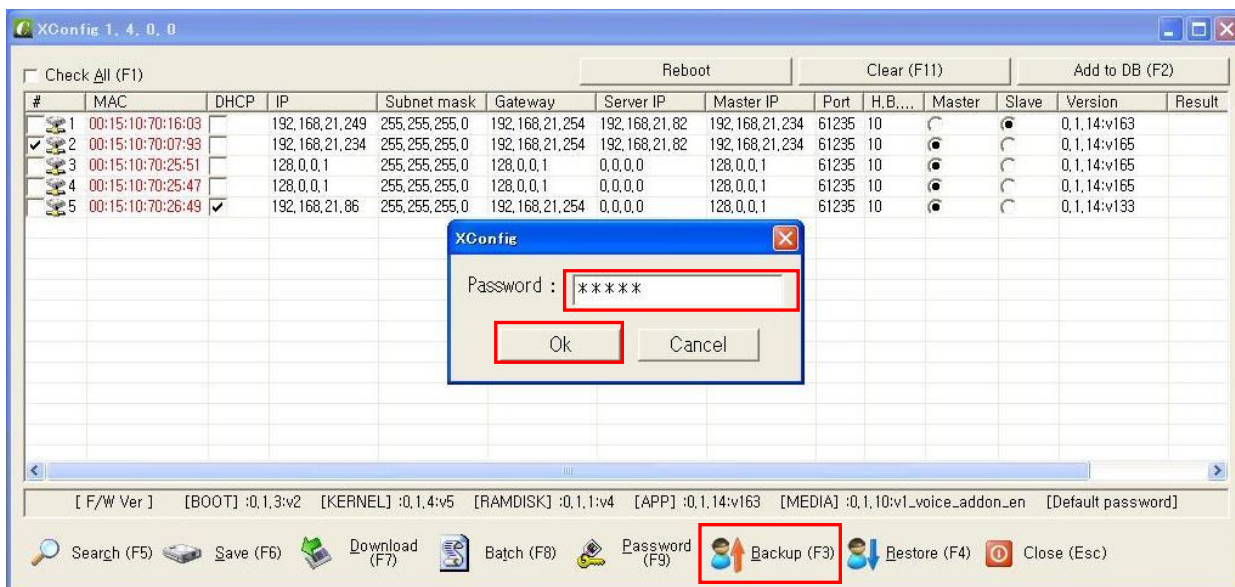
System[IP アドレス].dat ※VP-II Xのシステム設定情報

バックアップファイルには「.dat」という拡張子がつけられます。これは、XAgent Management Tool で作成されるファイル(「.tsdat」と同じです。

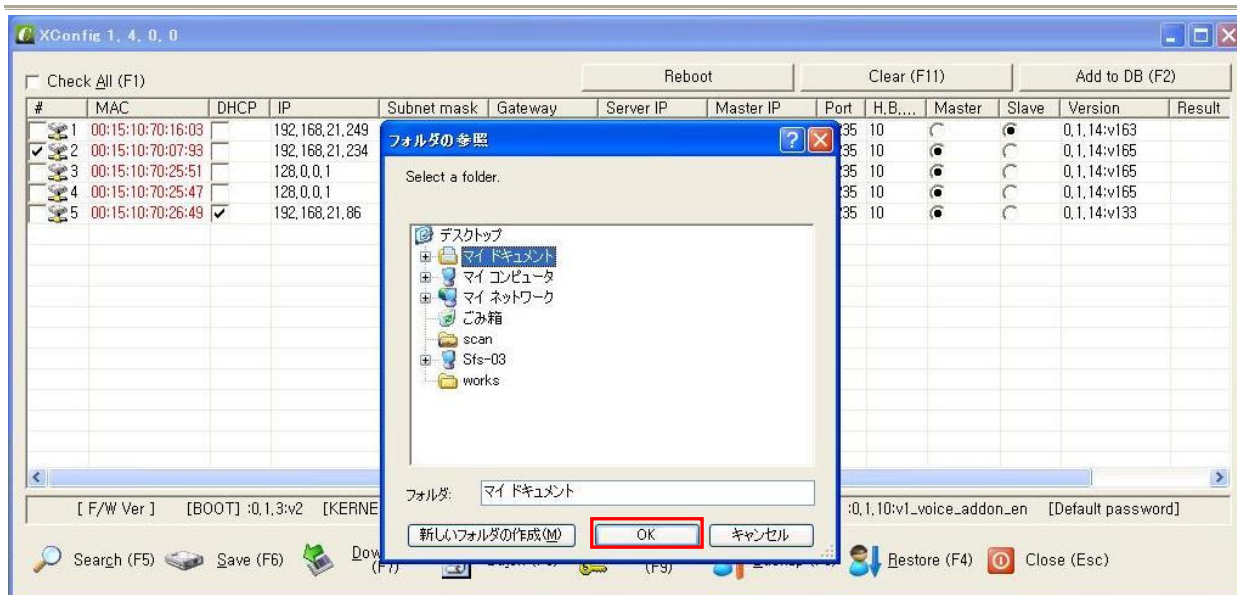
[Backup (F3)]や[Restore (F4)]を選択して、VP-II Xにある使用者データベース/VP-II Xのシステム設定情報のバックアップやリストアを開始することができます。この操作もパスワード入力する必要があります。



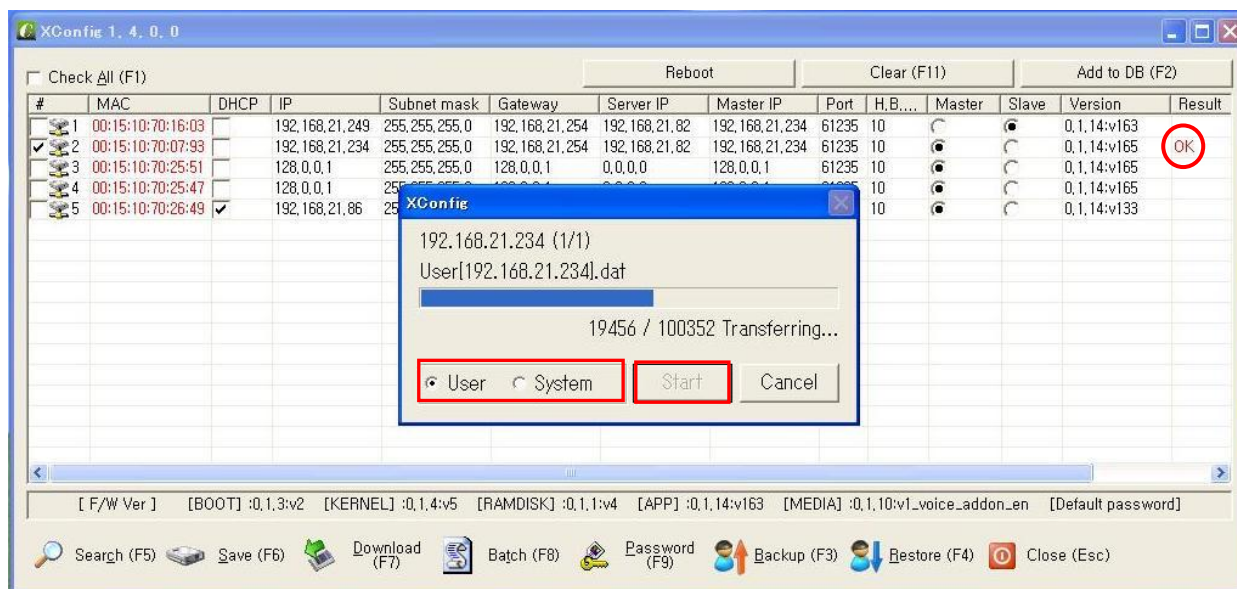
□ Backup (F3) バックアップ方法



チェックボックスをクリックして任意の VP-II X を選択してから[Backup (F3)]をクリックすると、パスワード入力ウィンドウが表示されます。パスワードを入力し、[OK]ボタンをクリックします。

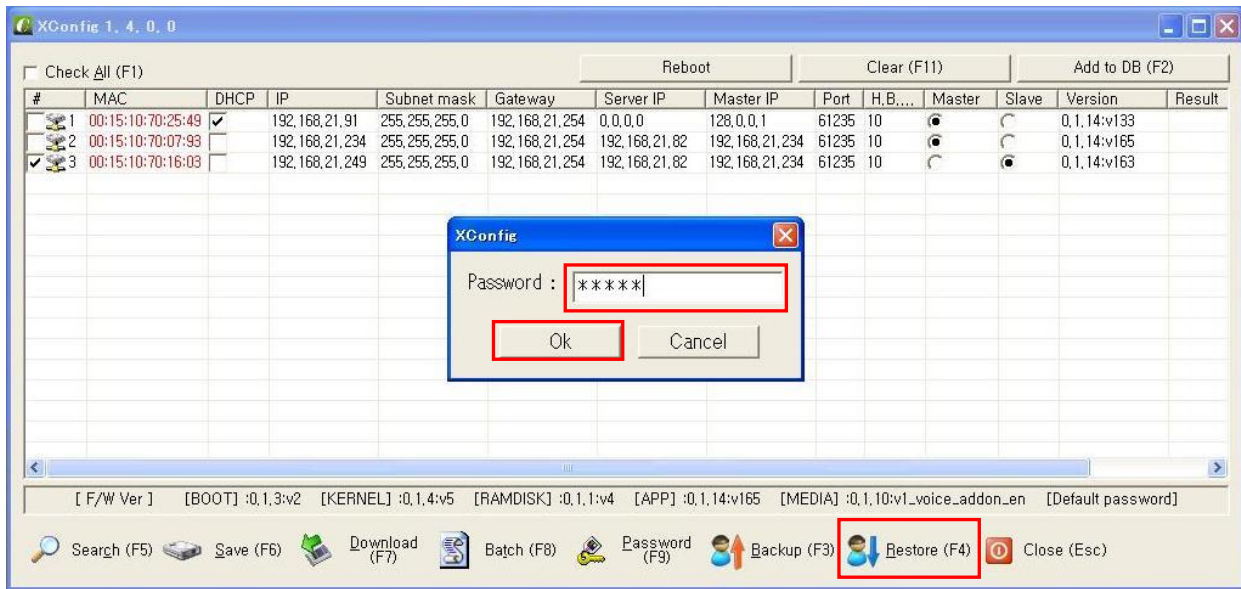


「フォルダの参照」ウィンドウが表示されます。バックアップファイルを保存するフォルダを任意で設定の上、[OK]をクリックします。

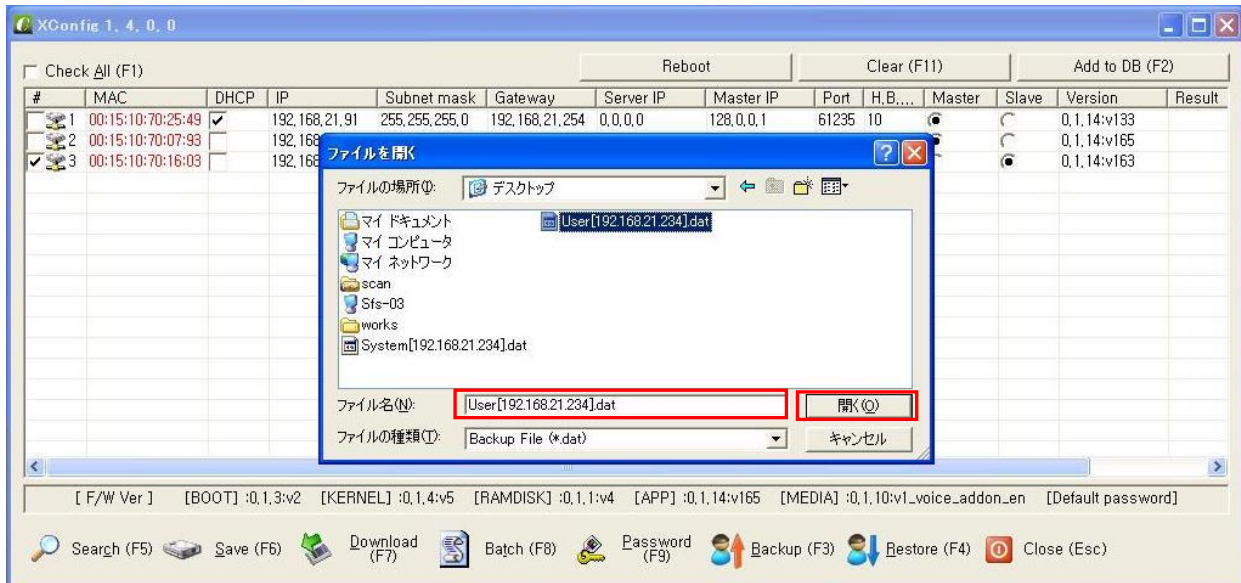


「Backup スタート」ウィンドウが表示されます。「User」／「System」のいずれかを選択して、[Start]ボタンをクリックすると、バックアップを開始します。バックアップに成功すると「Result」欄に「OK」と表示されます。

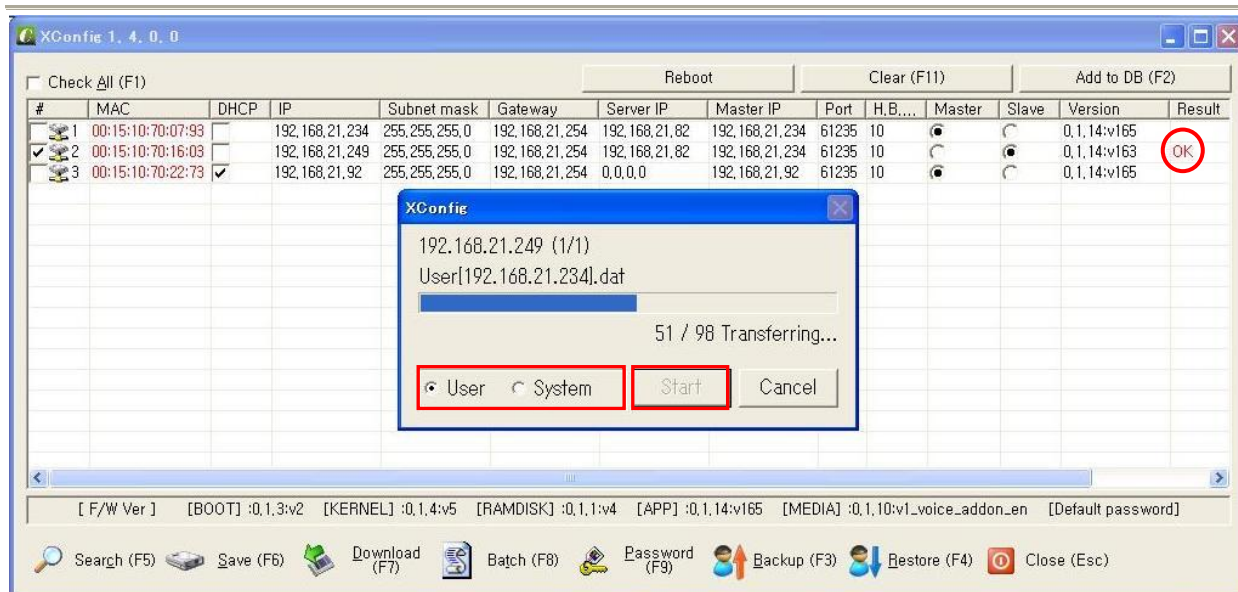
□ Restore (F4) リストア方法



チェックボックスをクリックして任意(複数台選択可能)の VP-II X を選択してから[Restore (F4)]をクリックすると、「パスワード入力」ウィンドウが表示されます。パスワードを入力し、[OK]ボタンをクリックします。



「フォルダを開く」ウィンドウが表示されます。バックアップファイル保存場所よりバックアップファイルを選択の上、「開く(O)」をクリックします。



「Restore スタート」ウィンドウが表示されます。「フォルダを開く」ウィンドウで選択したバックアップファイル「User」／「System」のいずれかを選択します。[Start]ボタンをクリックすると、リストアを開始します。リストアに成功すると「Result」欄に「OK」と表示され、自動的に VP-II X は再起動します。リストア開始時にファイル「User」／「System」の選択に誤りがあると「Result」欄に「Fail」とエラー表示されます。

Hand Vascular Pattern Recognition System

VP-II XGドアコントローラ

Hand Vascular Pattern Recognition System



設置&取扱説明書

Ver.1.5



はじめに

手の甲静脈認証システム VP-II X をお買い上げいただき、まことにありがとうございます。

このガイドは、VP-II XG ドアコントローラの設置と操作方法のためのガイドです。VP-II X のセットアップ、機能、ネットワーク設定に関する詳細は VP-II X 設置説明書と VP-II X 取扱説明書をご参照ください。なお VP-II X の各種取扱説明書は電子ファイルとして提供されます。

□ カスタマーサービス

設置済み製品の構成を追加または拡張する場合、または修理や保守が必要である場合は、設置担当者、または製品の販売店にご連絡の上、熟練した技術者の支援を得てください。テクニカルサポートやその他のサービスの詳細については、販売店にお問い合わせください。

株式会社 SYNCHRO

〒102-0073 東京都千代田区九段北 1-10-9 九段 VIGAS 5 階

Tel: 03-4570-3291 FAX: 03-4570-3292

電子メール: message@udc-synchro.co.jp

Web: www.udc-synchro.co.jp

□ 免責事項

本書に記載されている内容は情報提供のみを目的としています。Techsphere は、不正確または不完全な情報に対して、およびこれらの情報を信頼して行われた行為に対して、一切の責任を負いかねます。

注意:この説明書の内容は、製品の性能向上を反映するために、変更されることがあります。

□ 著作権について

本書は独占所有物です。参照以外の目的では使用しないでください。Techsphere Co., Ltd.はいかなる時点でも、この製品を変更また製造を停止する権利を保有しています。

改訂情報

- **V1.0: 2009 年 9 月**
 - 初版発行
- **V1.1: 2010 年 1 月**
 - VP-II X と VP-II XG のペアリング説明追加
- **V1.2:2010 年 6 月**
 - 接続ポートの詳細説明を追加
- **V1.3:2011 年 9 月**
 - 関連するイメージ図一部変更、追加
- **V1.4:2013 年 11 月**
 - VP-II XG ステータス LED 説明変更
- **V1.4:2017 年 12 月**
 - VP-II XG 付属品の説明追加

目 次

はじめに	2
改訂情報	3
1. VP-II XGドアコントローラ	5
2. 付属品	5
3. 設置	5
3.1 バックプレートとXGの設置	5
3.2 ポート接続	6
VP-II Xとの接続	8
3.3 ペアリング設定	9
3.4 ステータス LED	10
4. 通信データの暗号化	11

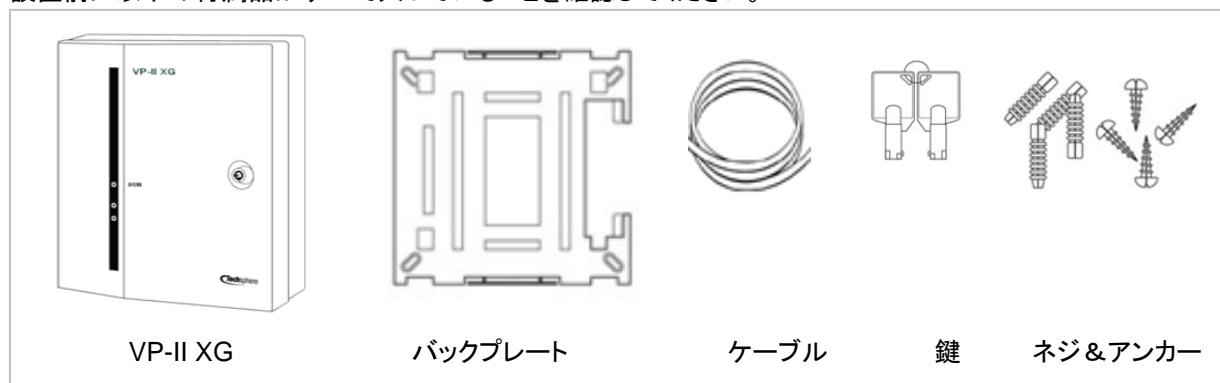
1. VP-II XG ドアコントローラ

VP-II XG は、VP-II 手の甲静脈認証装置で使用されるドアコントローラです。XG は RS232(または RS485、RS485 インターフェースを使用するには X と XG の両方にオプションの RS485 モジュールを取り付ける必要があります) 経由で VP-II X に接続されるもので、通常、ドアのセキュリティで保護されている側に設置されます。

VP-II XG 仕様	
電源	DC 12V~15V / 0.5A (AC アダプタまたは外部電源より供給)
使用温度／使用湿度	-15 ~ 50°C / 10 ~ 90%
重量／寸法	350g / 194x197x36.5mm

2. 付属品

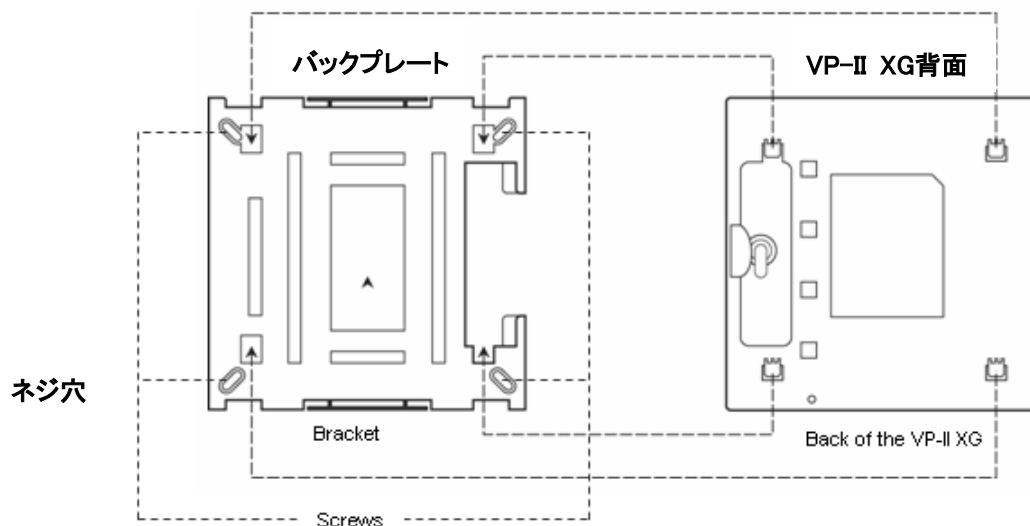
設置前に以下の付属品がすべて入っていることを確認してください。



3. 設置

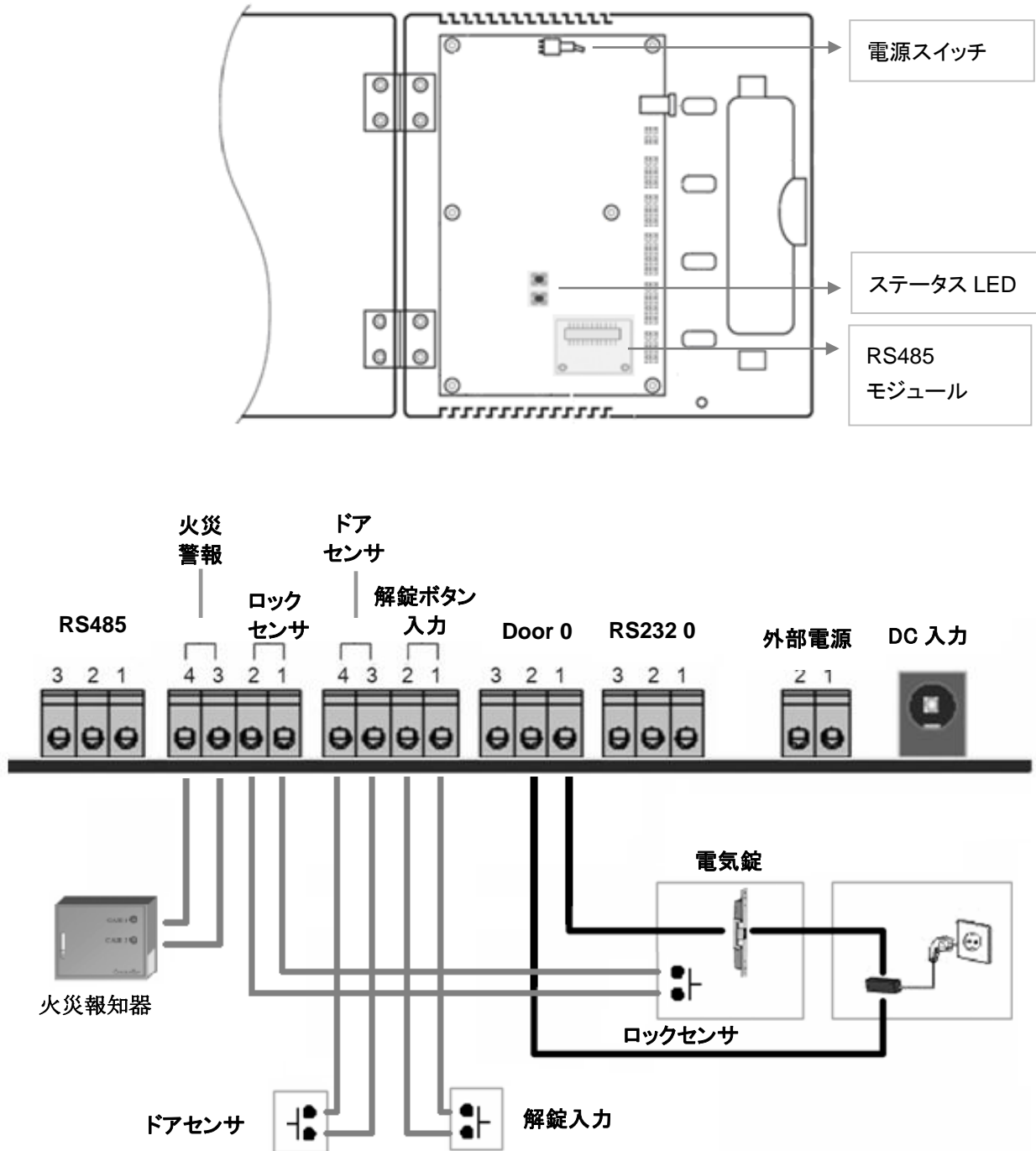
3.1 バックプレートと XG の設置

XG を設置するためのバックプレートを設置場所に置き、ケーブル通線口の位置を確認してから、穴を開けます。ネジを用いて、バックプレートを壁に固定します。その後、バックプレートに XG を、下の図に示すように上から下へ引っ掛けて取り付けます。



3.2 ポート接続

VP-IIX、ドアロックやドアセンサーとを接続するために XG の上部カバーを開けます。下図は、上部カバーが開いている XG の内部を表示しています。



□ リレー出力

XG は、電気錠を接続するための無電圧接点リレー出力を提供します。

XG 内部のリレーへの最大入力 は 24V、1A を超えないようにしてください。

N.O.(A 接)は常時開いており、ドアの解錠信号が有効であるときに閉じられます。

ポート No.	説明
1	N.O (常時開)
2	Common
3	N.C (常時閉)

ドア解錠の出力時間は VP-II X 管理者メニューおよび管理ソフト NetContol-X から設定可能です。

詳細は各種、取扱説明書をご参照ください。

□ RS232 / RS485

X と XG の距離が 15m を超える場合、RS485 インターフェースを使用できます。ただし、デフォルトでは RS485 モジュールはインストールされていないため、VP-II X と XG の両方への追加インストールが必要です。RS485 モジュールは別途提供されます。詳細は、製品の販売店にお問い合わせください。

□ 電源 入力

電源は DC ジャックまたは+12 V/ GND ポートのいずれかに供給することができます。必要な電源は DC 12V~15V、0.5A です。VP- II X 用の電源が長距離にはなる場合は VP-II X への RS232 接続を使用する場合、電源は VP-II X から供給することができますが RS485 を使用する場合は、外部電源を使用する必要があります。

□ J2 (ジャンパー-SW)

これは、VP- II XG のメモリ(ペアリング機能は、次の項目を参照)に格納されたペアリング情報をリセットすることです。ペアリング情報を消去するには、電源がオフのときに、ピンセットやクリップなどで J2 を短絡し、そして短絡したまま電源スイッチを ON にしてください。ステータス LED(RUN)は、ペアリング情報がリセットされたことを示すと数秒間緑点滅します。

□ 解錠ボタン、ドアセンサ、ロックセンサ、火災警報入力

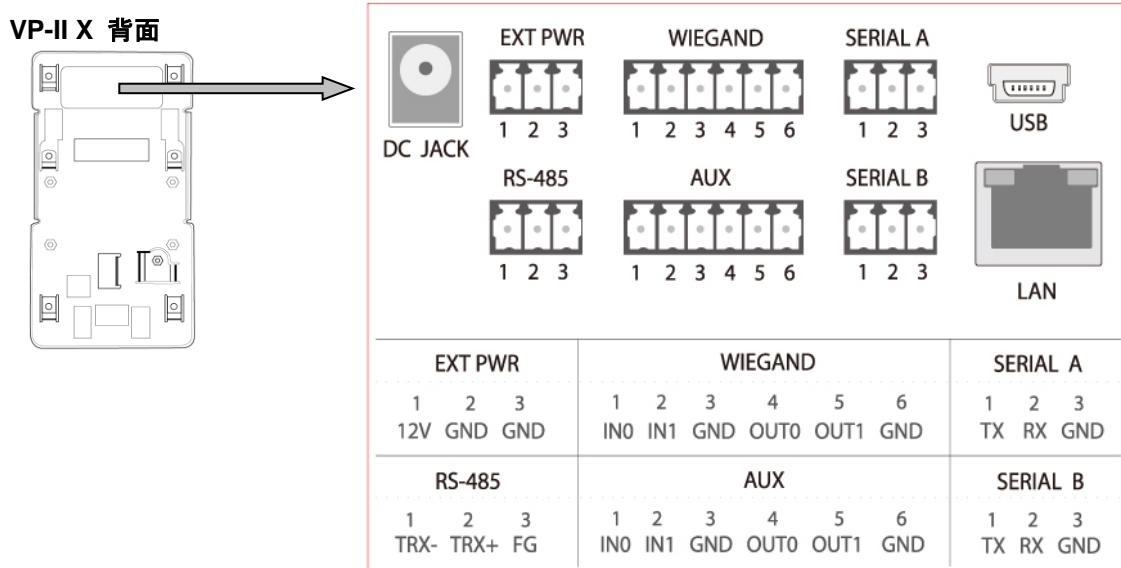
これらはデジタル入力ポートです。これらのポートに対する入力は無電圧接点でなければなりません。有電圧接点は使用しないでください。

** ロックセンサ: 電気錠が解錠または施錠されているかどうか電気錠の状態を検知します。

** ドアセンサ: ドアが開いているか閉じているかどうかドアの状態を検知します。

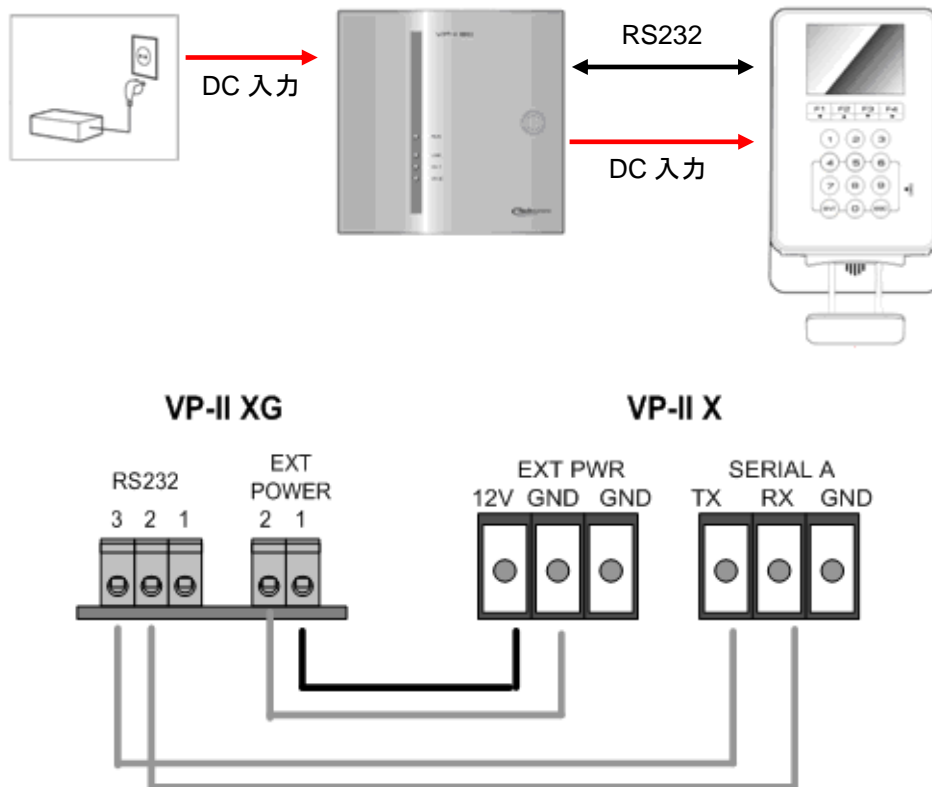
** 火災警報: 火災警報が入力されると電気錠は強制的に解錠します。

VP-II X との接続



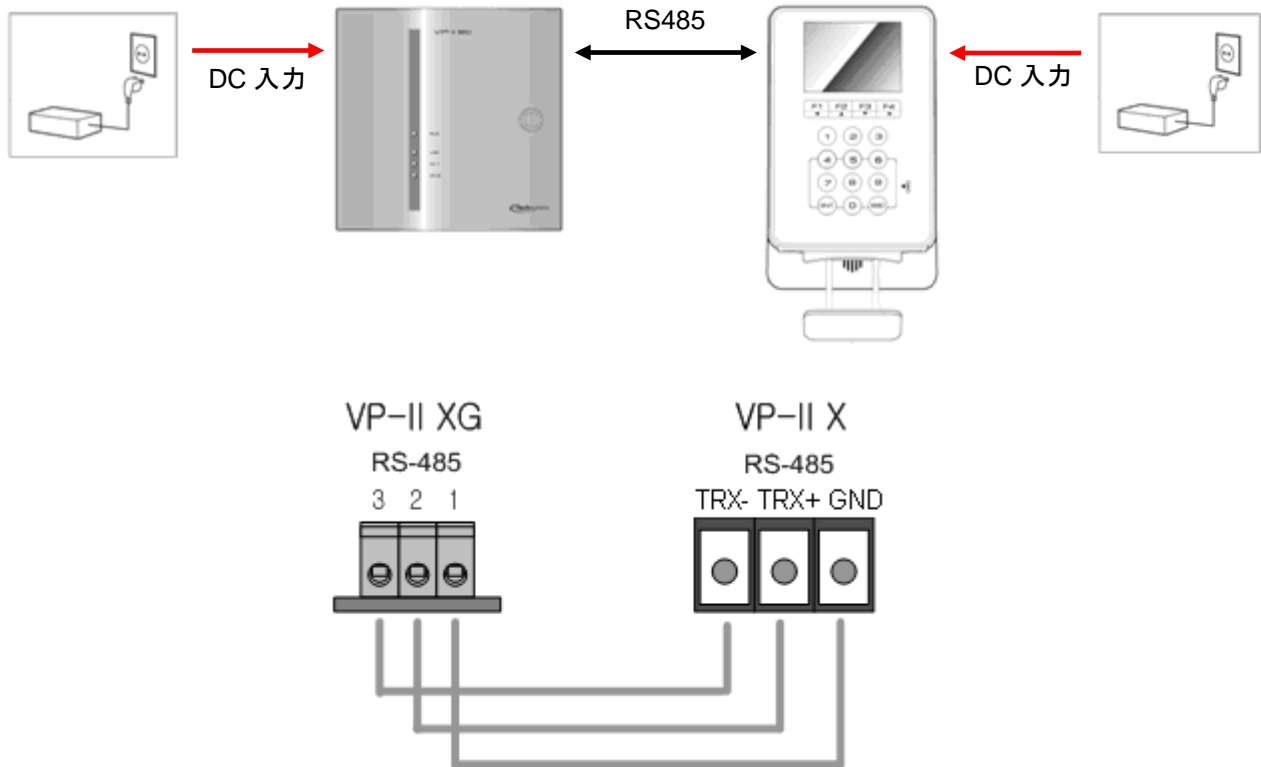
□ RS232 接続

VP-II X と RS232 接続を使用する場合、VP-II XG 経由で VP-II X へ電源を供給します。



□ RS485 Connection

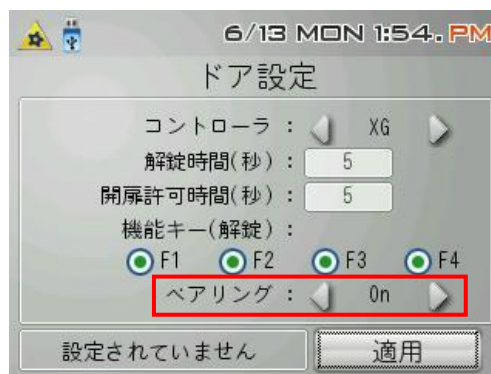
RS485を使用する場合はVP-II Xへの電源供給は長い距離があると使用できないため、外部電源を使用する必要があります。



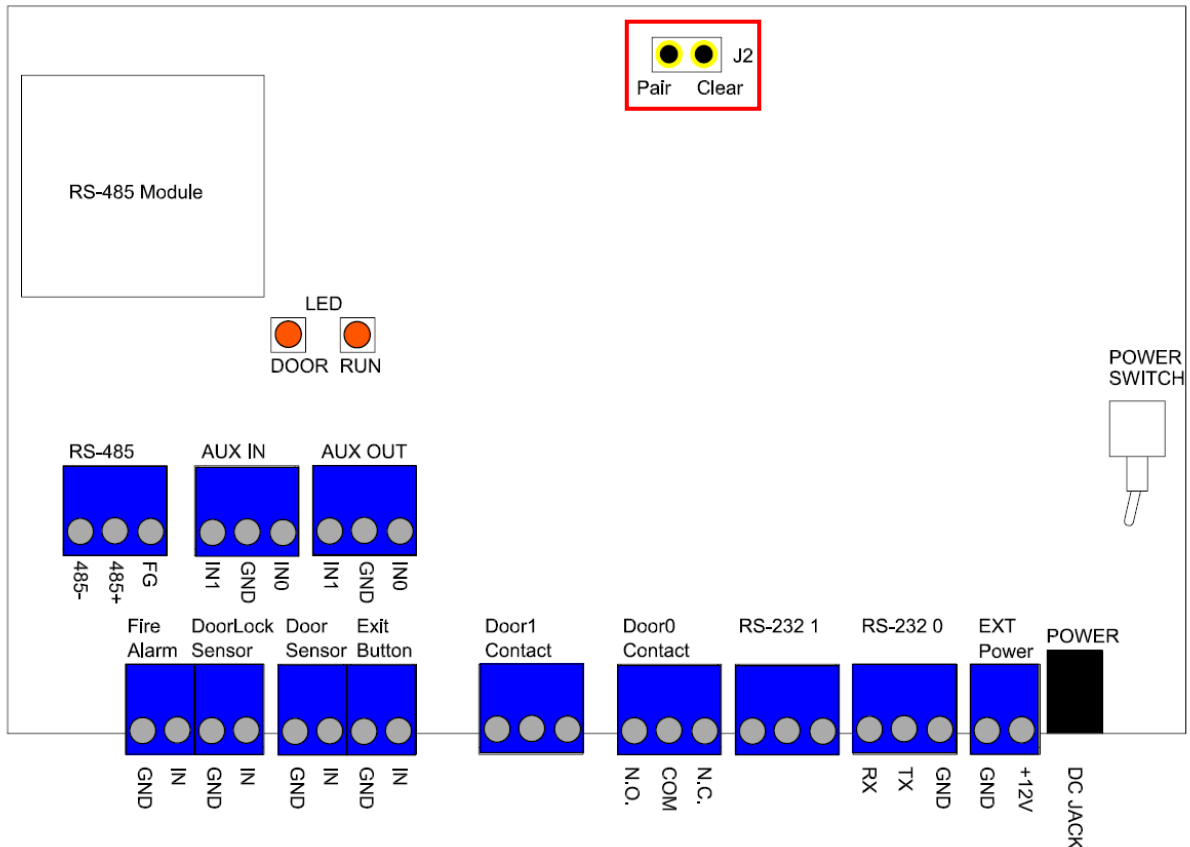
3.3 ペアリング設定

VP-II X と VP-II XG はペアリング設定することで他の VP-II X によって扉を解錠できないように設定することができます。例えば、誰かが認証を許可されていない VP-II X を認可されている別の VP-II X に取り替えて、使用者の使用者の認証により扉を解錠しようとした場合、VP-II XG は扉の解錠を受け付けません。VP-II XG はペアリング設定した VP-II X からのコマンドのみ受け付けます。VP-II XG および VP-II X 両方を設置後、VP-II X の管理者メニューによってペアリング設定を行うことができます。

管理者メニュー > 3. システム設定 > 5. ドア設定



ペアリング設定が有効時(On)には VP-II X は、VP-II X と XG 両方に納されるランダムキーを発生させます。キーは、どのようなコミュニケーションのためにもお互いを特定するのに使用されます。一度 VP-II X とペアリング設定された VP-II XG ペアリング設定が初期化されるまで、他のいかなる VP-II X とはペアリング設定できません。VP-II XG を初期化するにはニアブ基板上のジャンパースイッチ(J2)を短絡したまま電源を ON にしてください。



3.4 ステータス LED

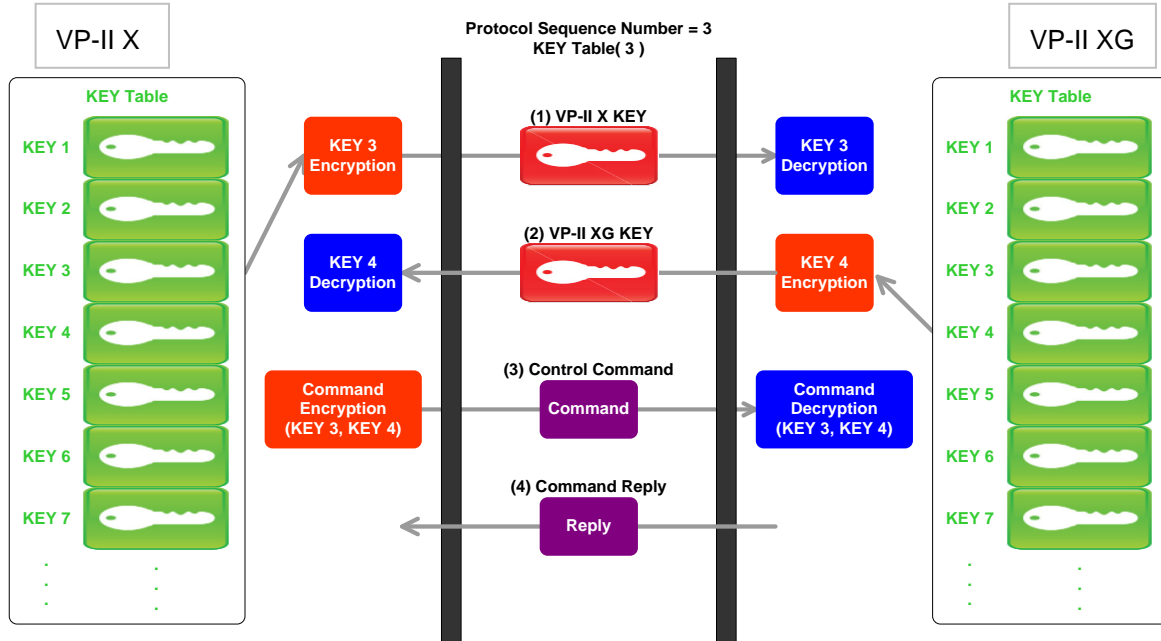
VP-II XG の状態を示す LED は以下で説明するように作動します。



LED	Status	
RUN	消灯	電源 OFF 時
	赤点滅	ペアリング未設定時
	赤/緑/橙点滅(高速)	ペアリング設定時(正常時)
DOOR	消灯	解錠信号未入力時
	橙点灯	解錠信号入力による解錠時

4. 通信データの暗号化

XG 間のすべてのデータ通信は、通信回線からデータをフックすることによってすべての可能なハッキングから防ぐために、安全に暗号化されています。



□ コミュニケーションシーケンス

- VP-II Xはメモリとランダム値で格納されたキーテーブルから組み合わせで生成された暗号化キーを送信します。
- VP-II XGは受信した暗号キーを解読してキーが有効であると確認します。キーが有効であるならXGは、また同じ方法で新しい暗号化されたキー(キーB)を生成して、VP-II Xに新しいキーを送ります。
- VP-II XはキーA、キーBと実行するコマンドを使用して制御コマンドを作成し、VP-II XGに作成された制御コマンドを送信します。
- VP-II XGはコマンドを実行して、VP-II Xに応答します。