IntraGuardian2+
Manager Professional

（Version 3.4 ～）

ユーザーマニュアル

第6版

2018年1月24日

日本シー・エー・ディー株式会社

はじめに

この度は、不正接続検知／排除システム IntraGuardian2+ Manager Professionalをご利用いただき、誠にありがとうございます。
本書ではIntraGuardian2+ Manager Professionalの操作、設定方法を説明いたします。インストール方法につきましては「インストールガイド」をご参照ください。

本書についてのご注意

- 本書の内容の一部でも無断転載することは禁止されています。
- 本書の内容は、将来予告なく変更することがあります。

お願いとご注意

- 本ソフトウェアの無断複製・解析は禁止されています。
- 本ソフトウェアに使用されている意匠、商標の無断使用は禁止されています。
- 本ソフトウェアの転用は禁止されています。
- 本ソフトウェアは日本国内の使用を前提として設計・開発・製造されていますので、海外では使用しないください。
- 本ソフトウェアは、一般的な情報通信回線用途として設計・製造されています。従って、生命、財産に著しく影響を及ぼすため高信頼性を要求される、制御・監視等のシステム（原子力発電設備、医療設備等の動作を制御または監視するシステム等）の用途では使用しないください。

知的財産権等

- IntraGuardian は日本シー・エー・ディー株式会社の登録商標（第5288137号）です。
- 本ソフトウェアに搭載されている不正接続検知／排除システムに関する著作権その他の知的財産権は、日本シー・エー・ディー株式会社が所有するものです。
- Windows, Internet Explorer は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

免責事項について

- 本ソフトウェアの使用または使用不能から生ずる一切の損害（情報内容の変化、情報 の喪失、事業利益の喪失、事業の中断、他製品・システムへの損害などを含む）に関して、当社は責任を負いかねますので予めご了承ください。
- 地震、雷、風水害、火災、第三者による行為、その他の事故、お客様の故意、過失、誤用、 その他の異常な条　件での使用により生じた損害に関して、当社は責任を負いかねますので予めご了承ください。
- 本ガイドの記載内容を守らないことにより生じた損害に関して、当社は責任を負いかねますので予めご了承ください。
- 当社指定外の機器、ソフトウェアとの組み合わせによる誤動作から生じた損害に関して、当社は責任を負いかねますので予めご了承ください。

ソフトウェア使用許諾契約

IntraGuardian2+ Manager Professional（以下、「本ソフトウェア」といいます）は、不正接続検知／排除システムIntraGuardian用の集中管理ソフトウェアです。
また、IntraGuardianは、日本シー・エー・ディー株式会社（以下、「NCAD」といいます）の商標です。

1. **使用許諾**
    1. 本ソフトウェアは、使用許諾されるものであり、販売されるものではありません。
    2. お客様には、お客様に設置されているIntraGuardianの集中管理を目的として、IntraGuardianとともに本ソフトウェアを使用する非独占的な権利が許諾されます。お客様は、当該目的以外では、本ソフトウェアを一切使用できません。
    3. お客様は、本ソフトウェアを改変または複製できません。本ソフトウェアをベースにしたソフトウェアを作成することもできません。

2. **著作権等**
    1. 本ソフトウェアに関する著作権その他の知的財産は、NCADが所有しております。
    2. 本ソフトウェアに関する著作権その他のいかなる知的財産もお客様に譲渡されるものではありません。
    3. お客様は、本ソフトウェアおよびその関連資料に使用されている著作権表示、商標その他の表示を除去できません。

3. **リバースエンジニアリング**
   お客様は、自身でまたは第三者を介して、本ソフトウェアのリバースエンジニアリング、逆コンパイル、逆アセンブルを行うことができません。

4. **使用中止**
   お客様がIntraGuardianを使用しなくなった場合、お客様はIntraGuardianの集中管理データを維持・管理する目的で本ソフトウェアを使用する以外では、本ソフトウェアを一切使用できません。

5. **非保証・責任の限定**
    1. NCADは本ソフトウェアに関して、その品質および性能に関する保証を含め、いかなる明示または黙示の保証も致しません。
    2. NCADは、本ソフトウェアの使用または使用不能から生じたお客様の損害等について一切責任を負いません。

6. **輸出管理**
   お客様は、本ソフトウェアに関し、日本の外国為替及び外国貿易法ならびに関係法令（以下、「法令等」といいます）を順守し、法令等に基づく許可およびNCADの承認なく、本ソフトウェアを直接または間接的に輸出（海外への持ち出しを含む）しないものとします。

7. **NCADの権利**
   お客様は、NCADが自己の名義で本契約に基づき権利を行使できることを了承します。

8. **管轄裁判所**
   本ソフトウェア契約に関し紛争が生じた場合には、東京地方裁判所を管轄裁判所とするものとします。

以上

日本シー・エー・ディー株式会社
〒161-0033 東京都新宿区下落合2-14-1 CADビル

目次

1. 管理画面へログイン・ログアウト

1-1. Webブラウザを起動

管理画面にアクセスするためにWebブラウザ（以下、ブラウザ）を起動します。本ソフトウェアをインストールしたPCのブラウザでも、本ソフトウェアとTCP/IPのネットワークでつながっている他のPCのブラウザでも構いません。

1-2. 管理画面へログイン

ブラウザのアドレス欄に以下のアドレスを入力して、本ソフトウェアにアクセスします。

※ xxx.xxx.xxx.xxx は本ソフトウェアをインストールをしたサーバーのIPアドレスになります。ネットワーク内でDNSが適切に管理されている場合、ホスト名を指定してもかまいません。

※ 10080 は本ソフトウェアをインストールした際に指定した「UI使用ポート番号」になります。（デフォルトは 10080）

アドレス（URL）	http://xxx.xxx.xxx.xxx:10080/

「**ID**」と「**Password**」を入力して［**ログイン**］ボタンをクリックし管理画面へログインします。

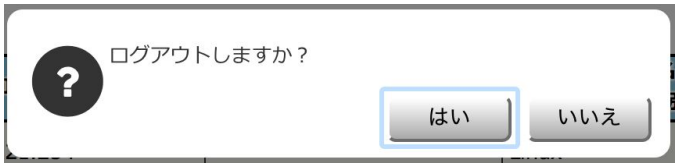
※ 現在は日本語のみ対応のため、「言語」は日本語固定です。

※「ID」と「パスワード」はインストール時に指定した内容になります。忘れた場合は本ソフトウェアのインストールをやり直してください。

1-3. 管理画面からログアウト

本管理画面での操作を終わる場合、右上にある「**ログアウト**」ボタンをクリックします。

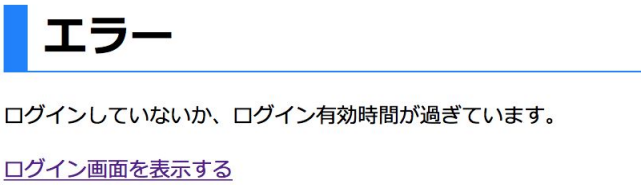
クリック後、右図のように確認ダイアログが表示されますので、「**はい**」をクリックします。ログアウト完了するとログイン画面に遷移しログアウト完了です。



1-4. ログインタイムアウト

何も操作しないまま一定時間を経過すると強制的にログアウトします。（画面は自動的に切り替わりませんが、次になんらかの画面を表示しようとすると、右のエラー画面が表示されます。）
「ログイン画面を表示する」をクリックするとログイン画面に戻ります。

ログイン有効時間を変更する場合は、「マネージャ設定」を確認してください。



2. メニュー

管理画面の上に常に表示されているのがメニューです。

メニューは作業内容によりグループ分けされ、トップメニューでグループを選択し、サブメニューで作業内容を選択します。

2-1. 通常メニューグループ

通常メニューグループは日常の運用作業で操作する項目です。メニュー部背景がブルー(青)色になります。

通常メニュー表示時は、左上に現在着目しているセクションの名前が表示されます。このセクション名をクリックすると、着目するセクションを切り替えることができます。

着目しているセクションで現在検知されている不正端末を確認したり、不正検知などの履歴を見る、登録端末の管理をする、セクションの管理をする、IntraGuardianの設定(監視設定)を変更する、といったことが行えます。

2-2. マネージャグループ

マネージャグループはマネージャ全体の動作設定を変更することができます。メニュー部背景がオレンジ(橙)色になります。

マネージャやIntraGuardianの動作状況の履歴を見たり、IntraGuardian2+ Manager Professional自身の動作設定をする、オペレータの登録をする、端末種別などの項目管理をする、IntraGuardianのファームウェアバージョンアップをする、外部システムとの連携処理をする、といったことが行えます。
なお、マネージャグループの各操作は後に述べる全権管理者だけが行うことができます。

2-2. メンテナンスグループ

メンテナンスグループは本ソフトウェアの運用を補助する機能です。メニュー部背景がグリーン(緑)色になります。

設定とデータのバックアップ・復元を行ったり、OUIコード(ベンダコード)データベースを更新する、IntraGuardianとの接続状況を確認する、ライセンスの登録をする、本アプリケーションのバージョンアップをする、本アプリケーションを強制再起動／終了する、といったことが行えます。
なお、メンテナンスグループの各操作は後に述べる全権管理者だけが行うことができます。

3. セクション管理

IntraGuardian2+ Manager Professionalでは、監視するネットワークを「セクション」と呼ぶ単位でまとめて管理をします。本章ではこのセクションの概念について説明し、実際にセクションを作成する方法を説明します。

3-1. セクションとは

端末登録を取りまとめる単位を「セクション」と呼びます（旧バージョンにおける「ネットワーク」の概念とほぼ同じになります）。セクションには、例えば「営業1課」「札幌支店1F」「本社会議室」などのように名前をつけることができます。セクションは、必要に応じて対応するIntraGuardianを割り当てることができます。IntraGuardianを割り当てる場合には、ネットワークアドレスなどの情報をセクションが持つことになります。

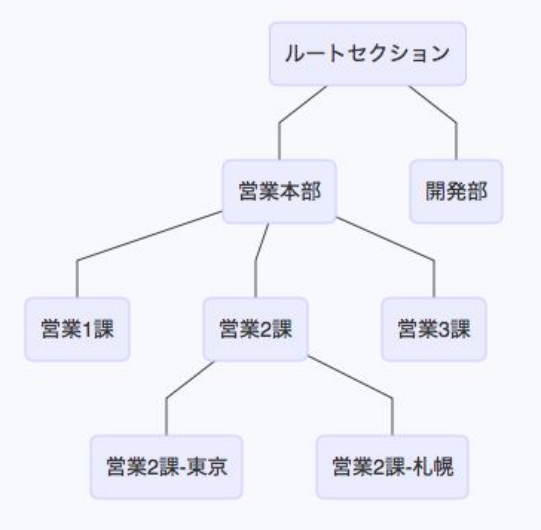
1つのセクションは0台または1台のIntraGuardianが対応することになります。1つのセクションに複数のIntraGuardianを割り当てることはできません。複数のIntraGuardianを束ねて管理したい場合には、次に述べるセクションの階層構造を利用します。

3-1-1. セクションの階層構造

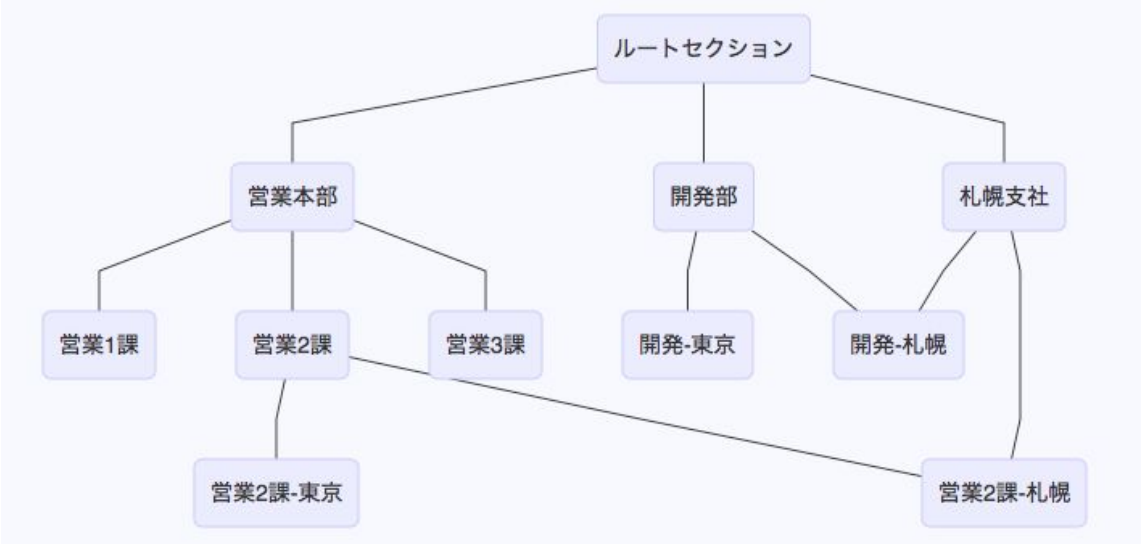
セクションは階層構造を持ちます。つまり、セクションの中に子セクションを任意の個数設置することができます。

また、セクションは必ず親セクションを1つ以上持ちます。例外は、すべてのセクションの祖先となる「ルート」セクションだけで、ルートセクションはシステム内に1つだけ存在し、削除することはできません。（デフォルトではルートセクションには「全体」という名前がつけられています。）

セクションの階層構造を図にすると、例えば右図のようになります。

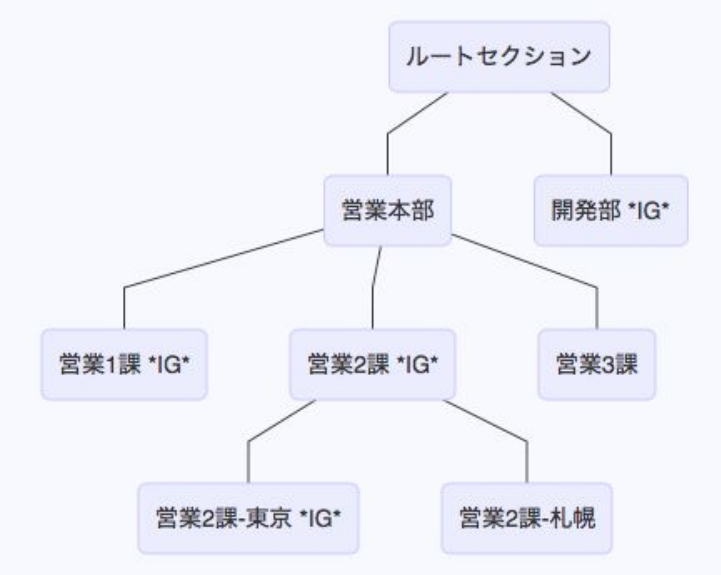


各セクションの親は複数設定することができます。（ただし、自分の子孫が親になるような循環関係は許されません。）つまり、上図のような木構造以外にもより複雑な構造を取ることができます。



3-1-2. 登録端末

各セクションには、任意の数の端末を登録することができます。端末の登録は、セクションの階層の下の方に継承されます。例えば、右図で「営業2課」に登録された端末は、「営業2課-東京」「営業2課-札幌」にも登録されているとして取り扱われます。
（右図中、”*IG*”の印はそのセクションにIntraGuardianが設置されていることを示します。）
つまり、「営業2課」に設置されたIntraGuardianには「営業2課」に登録された端末＋「営業本部」に登録された端末＋「ルートセクション」に登録された端末のすべての端末情報が登録されているものとして送信されます
同様に「営業2課-東京」に設置されたIntraGuardianでは、次のセクションのいずれかに登録された端末が登録されているものとして処理されます：「営業2課-東京」「営業2課」「営業本部」「ルートセクション」
（ただし、IntraGuardianの性能上の都合により、MACアドレス数として40,000件を超える端末情報は送信されません。）



登録セクション	端末名	端末種別	有効期限	ホスト名 ワークグループ	初検知日時 確認日時	MACアドレス ベンダ	現在IPアドレス 登録IPアドレス
営業2課	営業2課-1	Windows				00:04:AC:D9:45:31 IBM	
営業2課	営業2課-2	Linux				00:04:AC:D9:45:32 IBM	
営業2課	営業2課-3	Router				00:04:AC:D9:45:33 IBM	
営業2課	営業2課-4	Mac				00:04:AC:D9:45:34 IBM	
営業2課	営業2課-5	Windows				00:04:AC:D9:45:35 IBM	
営業2課	営業2課-6	Router				00:04:AC:D9:45:36 IBM	
営業2課	営業2課-7	Linux				00:04:AC:D9:45:37 IBM	
営業2課	営業2課-8	Windows				00:04:AC:D9:45:38 IBM	
営業本部	営業本部-1	その他				3C:D9:2B:E0:FC:E0 Hewlett Packard	
営業本部	営業本部-2	Windows				3C:D9:2B:E0:FC:E1 Hewlett Packard	
営業本部	営業本部-3	Windows				3C:D9:2B:E0:FC:E2 Hewlett Packard	
営業本部	営業本部-4	Router				3C:D9:2B:E0:FC:E3 Hewlett Packard	
全体	全体-1	Linux				60:03:08:9C:37:BF Apple	
全体	全体-2	Mac				60:03:08:9C:37:C0 Apple	

＜「営業2課」セクションでは、「営業2課」とその祖先のセクションに登録された端末が登録されているとみなされる＞

一つの端末を複数のセクションに登録するということはできません。複数のセクションで利用できるようにしたい端末がある場合には、それらのセクションを統括する親セクションを作成し、その親セクションに対して端末を登録してください。

3-1-3. 不正端末

IntraGuardianで検知された不正端末は、セクション単位で一覧することができます。不正端末については、登録端末とは逆にセクションの上の方向に継承します。

例えば、営業2課セクションで不正端末の一覧を表示すると、営業2課のIntraGuardianと営業2課−東京のIntraGuardianで検知されている不正端末が表示されます。同様に、営業本部セクションで不正端末の一覧を表示すると、営業2課セクションの不正端末一覧に加えて、営業1課のIntraGuardianで検知されている不正端末も表示されます。

セクション	MACアドレス ベンダ	IPアドレス 別IPアドレス	ホスト名 ワークグループ	OS名 OS種別	検知日時 確認日時	保留時間	状態
営業1課	3C:D9:2B:D3:AA:22 Hewlett Packard	192.168.52.42			本日 23:24 本日 23:55	0	検知中
営業2課-東京	3C:D9:2B:F3:B7:70 Hewlett Packard	192.168.100.212	HOST01 WORKGROUP	Windows	本日 23:29 本日 23:55	0	排除中
営業2課-東京	3C:D9:2B:2E:FB:80 Hewlett Packard	192.168.100.88	HOST08 WORKGROUP	Windows	本日 23:22 本日 23:55	0	排除中

＜「営業本部」セクションでは、その子孫のセクションのいずれかで検知されている不正端末が表示される＞

3-2. セクション登録

インストール直後の状態では、ルートセクション(「全体」セクション)しか存在しません。複数のIntraGuardianを管理したい場合には、まずセクションを登録しなければいけません。セクションを作成しないとIntraGuardianの割当をすることもできません。

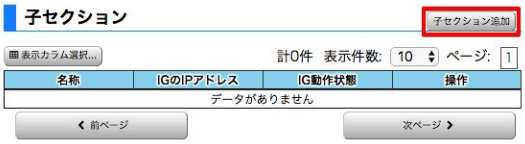
まずはトップメニューの「**通常メニュー**」をクリックします。

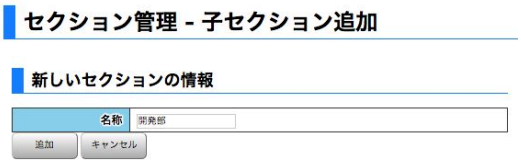
サブメニューの「**セクション管理**」をクリックし画面を表示します。

セクション追加を行うためには、セクション追加を行いたい親セクション(一つ上の階層)を指定します。(インストール直後の場合、ログイン直後に自動的に「全体」セクションが選択されていますので、そのまま全体セクション内に子セクションを追加してください。)

セクション管理画面にある「子セクション追加」ボタンをクリックします。

※セクションの追加は「子セクション追加」ボタン以外からは行えません。





追加したい子セクションの「**名称**」を入力し、「**追加**」ボタンをクリックしてください。

なお、8文字程度以下にしておくと、画面表示が綺麗にまとまります。

< 制限事項 >

名称	制限事項
名称	1文字以上、99文字以下で入力。既存セクション名との重複不可。

3-3. 着目セクションの切り替え

通常メニューグループの操作はすべて「現在着目しているセクション」に対して行います。現在着目しているセクションは、画面の左上に表示されています。

着目セクションを変更する方法は3つあります。やりやすい方法をご利用ください。

左上のセクション名をクリックする

左上に表示されている「現在のセクション名」をクリックすると、右図のようなセクションを切り替えるウィンドウが表示されます。
このウィンドウでセクション名をクリックして、切り替えてください。

セクション階層図のセクション名をクリックする

セクション階層の図の中のセクション名をクリックすると、そのセクションに切り替わります。
ただし、セクションが多数あったり階層構造が複雑である場合にはすべてのセクション名が表示されているわけではありませんので、選択できないことがあります。

子セクションのセクション名をクリックする

子セクションに選択を切り替える場合には、子セクションの一覧表の1行をクリックしても切り替わります。
子セクション数が多数ある場合にはページ切り替えをするなどして切り替えたいセクション名を表示してからクリックしてください。

3-4. セクション階層表示

セクション階層表示部はお使いの環境で見やすくなるように調整することができます。

セクション階層の「**表示設定**」をクリックすると、左図のようなウィンドウが表示されます。
このウィンドウ内のパラメータを調整して、見やすい状態を作ってください。

項目	設定内容
表示形式	Type-A： ルートセクションから現在のセクションまでと現在のセクションの子セクションを表示します。現在のセクションと関係があるセクションだけを表示するので、セクションの階層が複雑な時には見やすくなります。 Type-B： 現在のセクションの上位2階層と現在のセクションと同階層のセクション、及び子セクションを表示します。上位の階層の表示が制限されるので、セクション階層が深い場合に見やすくなります。 Type-C： 全セクションを表示します。セクション数が少ない場合にはすべてが一覧できるので見やすくなります。
最大行数	縦に並べて表示するセクションの最大数。
上位セクション段数	現在セクションの上位いくつのセクションまで表示するか。Type-Bでのみ有効です。
セクション間隔	セクション間の距離。
セクション名余白	セクション名とその周りの線との間の距離。
文字サイズ	セクション名表示に用いる文字の大きさ。

なお、この設定はオペレータ毎に保存されます。

3-5. セクション名称の変更

セクション名称の変更をしたい場合は、変更したいセクションを選択した状態でセクション管理画面を表示します。自セクションの「**名称**」から変更可能です。

名称を変更後、「**変更**」ボタンをクリックで完了です。
※入力の制限事項はセクション追加と同様になります。

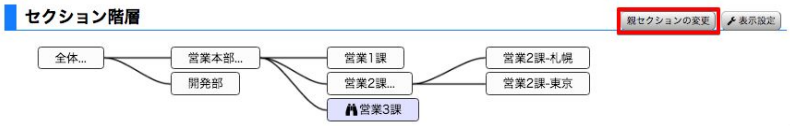
3-6. セクションの削除

セクションの削除は、セクション追加と同様に親セクションを指定して行います。まずは、親セクションを指定しセクション管理を表示します。子セクションの一覧から削除したいセクションの「**削除**」ボタンをクリックします。

確認画面が表示されるので、「**はい**」を選択すると削除完了です。

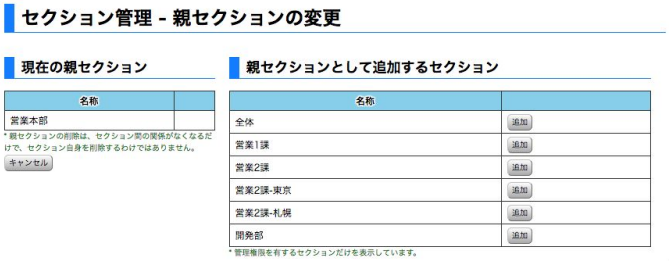
3-7. 親セクションの変更

親セクションを変更する場合は、変更したいセクションのセクション管理画面にある「**親セクションの変更**」ボタンをクリックします。



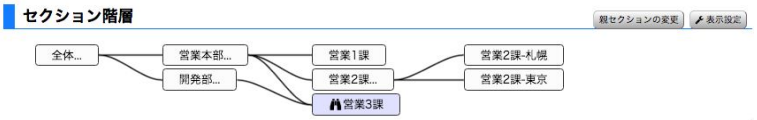
親セクションを追加する場合は、「**親セクションとして追加するセクション**」にある「**追加**」ボタンをクリックします。

また、親セクションを削除する場合は、「現在の親セクション」にある「**削除**」ボタンをクリックし完了です。



※関係が重複する場合は自動的に親セクションに登録されているセクションの差し替えが行われます。

例として、営業3課の親セクションに開発部を追加すると次のようになります。



4. IntraGuardianの接続

前章までにセクションの準備が整いましたので、ここではIntraGuardiianとの接続を行います。
IntraGuardian本体の管理画面を使って本マネージャに接続するための設定をしたのち、本マネージャの管理画面を使って接続を受け付ける設定をします。

4-1. IntraGuardianから本ソフトウェアへの接続設定

※IntraGuardian本体のバージョン3よりも古いファームウェアは、本ソフトウェアとの通信をサポートしておりません。

IntraGuardian本体の管理画面にWebブラウザでアクセスし、ログインします。
設置設定画面を開き、「**管理マネージャを使用する**」をクリックすると右図の設定画面が表示されます。
管理マネージャ種別は「**管理マネージャ Ver.3系**」を選択し、管理マネージャアドレスに本ソフトウェアの「**IPアドレス:管理画面にアクセスするポート番号**」を指定してください。
ポート番号の指定は、セットアップ時に指定したUI使用ポート番号になります。ポート番号を指定しなくてもほとんどの機能は正常に動作しますが、利用申請機能が正しく動作しなくなるためご注意ください。
なお、この画面に表示されている「**データベース保存場所**」は、のちにマネージャと接続した時点で自動的に正しく設定されますので、現時点ではどのような設定になっていても構いません。

入力を終えたら、**確定**ボタンをクリックして、10秒ほどお待ちください。

4-2. 接続状況確認

IntraGuardian本体での設定を終えると、IntraGuardian本体は本プログラムへの接続を試み始めます。
IntraGuardian本体からの接続要求が本プログラムに届いているかどうかは、**メンテナンス**メニューの**接続状況**画面をみるとわかります。
接続状況画面を開いたら、「接続要求中のみ」のラジオボタンをクリックしてください。

すると、上記のように接続を試みているIntraGuardianの一覧が表示されます。(この時点ではまだ通信を開始していないため、IntraGuardianの型式名などが不明ですが、これで正常な状態です。)

万が一、IntraGuardianからの接続要求が本プログラムに届いていない(上記一覧に表示されない)場合は、次の点を確認してください。

1. IntraGuardian本体は正しく本マネージャと接続する設定になっていますか？(「管理マネージャ Ver.3系」が選択されていますか？ IPアドレスは間違っていませんか？)
2. IntraGuardian本体の設置設定(特に「ゲートウェイ」の設定)は正しく設定されていますか？
3. IntraGuardianから本マネージャまで、ネットワーク的に正しく接続されていますか？(IntraGuardian本体は本マネージャの 17777 番ポートにTCP接続をします。このソケットを途中で遮断するネットワーク機器などは存在しませんか？)

4. 本マネージャを稼働しているWindows上でセキュリティ監視ソフトが動作していませんか？（上記の通り、本プログラムは17777番ポートのTCP通信を受信します。これをブロックするようなソフトウェアが動いていませんか？）
5. 当該IntraGuardianはすでに本プログラムで登録済み（割り当て済み）ではありませんか？（この場合「接続中のみ」を見ると表示されているはずです。）

なお、旧バージョンのIntraGuardian2 Managerとは異なり、マネージャからIntraGuardian本体へのTCP接続は発生しませんので、IntraGuardian本体はNATの内側にあっても構いません。

4-3. IntraGuardian割り当て

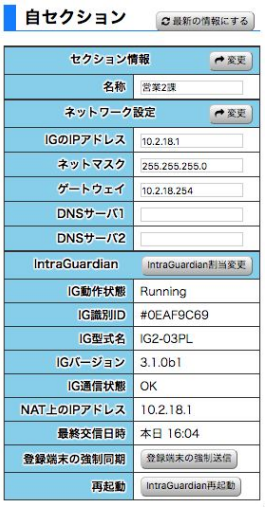
続いて検知／排除の動作をさせるためにIntraGuardianをセクションに割り当てます。
まず通常メニューの**セクション管理画面**を表示し、割り当てたいセクションを選択します。この画面の自セクションの「**IntraGuarian新規割当**」ボタンをクリックします。

※ すでに本セクションにIntraGuardianが割り当たっている場合には、ボタン名が「IntraGuardian割当変更」になります。

画面が「セクション管理 – IntraGuardian割り当て」に変わり、現在、接続要求中のIntraGuardianが一覧に表示されます。
IPアドレスから登録するIntraGuardianを判別し、クリックします。その後「**新規割当**」ボタンをクリックします。

※「NAT上のIPアドレス」とは、本プログラムから見た IntraGuardianのIPアドレスです。通常はIGのIPアドレスと同じアドレスが表示されますが、IntraGuardianと本マネージャとの間にIPアドレス変換を伴うルータなどが入っている場合には異なるアドレスとなることがあります。
また、IntraGuardian2 EX（VLAN対応版）の場合、NAT上のIPアドレスにはIntraGuardian本体がゲートウェイとして使っているネットワークセグメントのアドレスが表示されます。

割当が完了すると、自セクション欄にIntraGuardianの情報が表示されます。右図のように細かな情報が表示されていれば登録完了です。
なお、通信を開始してから全情報を正しく取得し終わるまで1-2分かかることがあります。「IG通信状態」が「OK」になっていない場合、1分ほど待ってから「最新の情報にする」をクリックしてみてください。



4-4. 割り当て中のIGの設定の同期について

セクションに割り当てられたIntraGuardianの動作および端末登録は本ソフトウェアで設定したものと同期されます。
また、割り当て中のIntraGuardianは以下のように動作します。

- IntraGuardian本体の管理画面から端末の登録、削除および編集は行えません。常に本ソフトウェアで登録した端末情報が用いられます。
- 本ソフトウェアによる設定が優先されます。そのため、IntraGuardian本体の管理画面から設定を変更しても、設定同期の際に本ソフトウェアで設定した通りに上書きされます。
  ただし、IntraGuardianが本プログラムに接続するために必要な最低限のネットワーク設定項目（IPアドレス、ネットマスク、ゲートウェイ）だけは、IntraGuardian本体の設定が優先されます。

なお、IntraGuardianの設定内容は、次の場合に本ソフトウェアからIntraGuardian本体に送信されます。

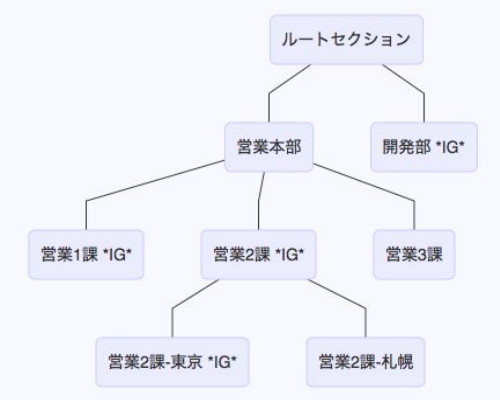
- IntraGuardianと本ソフトウェアが通信を開始した時（何らかの理由で通信接続をやり直した時を含む）
- 本ソフトウェアで当該IntraGuardianの設定（監視設定）を変更した時
- 定期的なステータス確認において設定の不整合を検出した時（IntraGuardian本体で設定を変更した等）

5. 監視設定

通常メニューの**監視設定**画面を使うと、指定セクションとその子孫セクションに設置されているIntraGuardianの設定を一度に変更できます。

5-1. 監視設定における操作方法

監視設定画面では、**指定セクションに設置されているIntraGuardianの設定**と、**指定セクション以下のセクションに設置されているIntraGuardianすべての設定**を変更することが可能です。そのため、画面は設定状態により4通りに変化いたします。
本節の説明では便宜的に右図のセクション構成を用いて説明を進めます。図中、"*IG*"と書かれているセクションが、IntraGuardianが設置されているセクションです。



5-1-1. 指定セクションに設置されていて、子孫セクションには1つも設置されていない時

右図は、**指定セクションにIntraGuardian が設置されていて、指定セクションの子孫セクションにはIntraGuardianが設置されていない**時の表示です。
前述のセクション構成の例では、「開発部」「営業1課」「営業2課-東京」がこのケースに当てはまります。
この場合、操作した設定は指定セクションに設置されたIntraGuardianの設定として利用されます。

5-1-2. 指定セクションには設置されていないが、子孫セクションには設置されている時

右図は、**指定されたセクションにはIntraGuardianが設置されておらず、指定セクションの子孫セクションのいずれかにIntraGuardianが設置されている**時の表示です。
前述のセクション構成の例では、「ルートセクション」「営業本部」がこのケースにあてはまります。
この場合、操作した設定は指定されたセクションの子孫セクションに設置されているIntraGuardianすべてに適用されます。
指定されたセクション以下に複数のIntraGuardianが存在した場合すべてのIntraGuardianの設定が更新されますのでご注意ください。
斜めの鎖のマークは、対象IntraGuardianすべてで設定が同一になっていることを示しています。設定が全て同じになっていない項目については、切れた鎖のマークが表示されます。

5-1-3. 指定されたセクションに設置されていて、子孫セクションにも設置されている時

右図は、**指定セクションにIntraGuardianが設置されていて、指定セクションの子孫セクションのいずれかにもIntraGuardianが設置されている**時の表示です。
前述のセクション構成の例では、「営業2課」がこのケースにあてはまります。

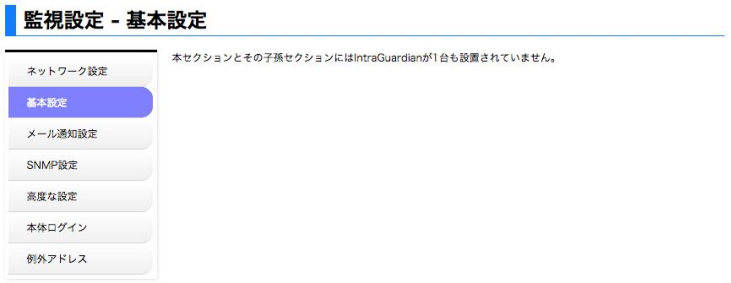
この場合、「**個別更新**」を選択・クリックすると指定されたセクションのIntraGuardianのみ設定が変更ができ、「**全体更新**」を選択・クリックすると指定されたセクションを含めて子孫セクションに設置されたIntraGuardianの設定がすべて変更されます。

斜めの鎖のマークは、対象IntraGuardianすべてで設定が同一になっていることを示しています。設定が全て同じになっていない項目については、切れた鎖のマークが表示されます。

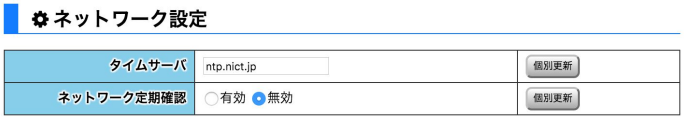
5-1-4. 指定されたセクションにも子孫セクションにも設置されていない時

右図は、**指定セクションにも、その子孫セクションにもIntraGuardianがまったく設置されていない**時の表示です。
前述のセクション構成の例では、「営業3課」「営業2課−札幌」がこのケースにあてはまります。

この場合、監視設定画面では何も行うことができません。



5-2.（監視設定）ネットワーク設定



IntraGuardian本体がネットワークにアクセスする際の設定を更新できます。

※ IntraGuardianが用いるIPアドレス等の設定は本画面から変更できません。変更する場合は「セクション管理」から行ってください。

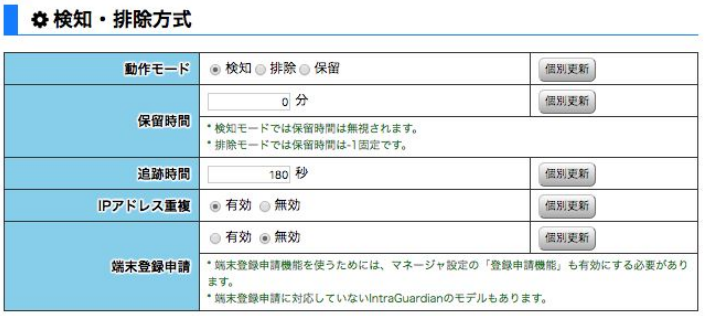
タイムサーバ	時間同期するサーバを指定します
ネットワーク定期確認	有効に設定するとゲートウェイアドレスに定期的にpingを送信し応答がなければネットワークインターフェースを再起動します

※ 詳しい各設定項目内容についてはIntraGuardian本体のスタートアップガイドをご参照ください。

5-3.（監視設定）基本設定

IntraGuardianの基本動作についての設定を更新できます。

5-3-1. 検知・排除方式



ここではIntraGuardianの検知・排除の動作を設定することができます。

動作モード	「検知」「排除」「保留」から動作を選択します
保留時間	動作モードが保留設定時に通信を許可する時間を指定します
追跡時間	検知した端末の有効時間を設定します
IPアドレス重複	排除時にIPアドレスを重複させて排除するかを指定します
端末登録申請	端末登録申請を利用するかどうかを指定します **※この設定とは別にマネージャ設定で端末登録申請機能を有効にする必要があります**

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-3-2. IPアドレスの取り扱い

IPアドレスに関する動作を設定することができます。

IPアドレス監視	IPアドレス監視を有効にすると登録されたIPアドレス以外を利用できないようにします

サブネットフィルタ	サブネットでフィルタリングするかしないかを指定します
例外IPアドレス	特定のIPアドレスの機器は不正として扱わない機能（例外IPアドレス）を使用するかしないかを指定します
GWのIPアドレスを例外扱い	ゲートウェイのIPアドレスを例外IPアドレスとして扱うかどうかを指定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-3-3. ホスト名検出

IntraGuardianで検知した端末のホスト名を検出する方式を指定します。

DNS利用	DNSによる名前解決を行うかどうかを指定します
優先プロトコル	DNS利用が有効の場合、NetBIOS(NBNS)又はDNSで見つけた名前のどちらを優先使用するか決定します ***DNSを選択した場合、ワークグループ名は空欄になります**
OS検出	OSの種類判別を行うかどうかを指定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-3-4. 巡回機能

IntraGuardianがネットワークを巡回監視する際のパラメータの設定を指定します。

巡回監視	セグメント内を定期的に巡回監視する機能を有効にするか選択します
送信間隔	ARPリクエストパケットの送信間隔を設定します **※極端に小さな値はネットワークへの負担を高めます。5ミリ秒以上を設定してください**
巡回実行間隔	巡回を終えた後に次の巡回を開始するまでの間隔を指定します
自サブネットの巡回	ネットワーク設定で指定したサブネットの巡回を行うかどうかを指定します
追加巡回範囲	自サブネット以外で巡回を行う場合にIPアドレスをレンジ指定します。**※巡回するIPアドレス範囲は最大10個指定することができますが、巡回数（巡回IPアドレス数）が65535を超えることができませんのでご注意ください。**

5-4.（監視設定）メール通知設定

IntraGuardianから通知で利用するメールを指定します。

※ 本項目の設定はIntraGuardian本体から送信するメールアドレスの設定です。本ソフトウェアからの通知設定とは異なるもののためご注意ください。

5-4-1. メール通知

IntraGuardian本体からメール通知をする際のパラメータです。

メール通知	メール通知を有効/無効化します
メール件名	通知メールの件名を設定します
言語	メール文に用いる言語を指定します
SMTPサーバ	メール配信に利用するSMTPサーバのアドレスを指定します
ポート番号	SMTPサーバで使用するポート番号を指定します(通常25)
送信元	通知メールを配信する際の送信元メールアドレスを指定します
SSL利用	メール送信時のSSL（TLS）利用方法を指定します
認証方式	メール配信に利用するSMTPサーバの認証方式を指定します
POP3サーバ	POP before SMTPを使って認証する際に利用するPOPサーバのアドレスを指定します
ポート番号	POP before SMTPを使って認証する際に利用するPOPサーバのポート番号を指定します(通常110)
アカウント	認証に使うユーザーアカウントを設定します
パスワード	認証に使うパスワード設定します
メール集約時間	本項目で指定された時間内にメール送信イベントが発生した場合、集約されます
再送待ち時間	送信に失敗した際に再送まで待つ時間を設定します
最大再送回数	送信に失敗した際に再送する回数を設定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-4-2. IPアドレス変化

検知した端末が使っているIPアドレスが変化した時にメール通知を発行する機能についての設定です。

IPアドレス変化通知	IPアドレス変化通知メールを有効/無効化します
メール件名	メールの件名を設定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

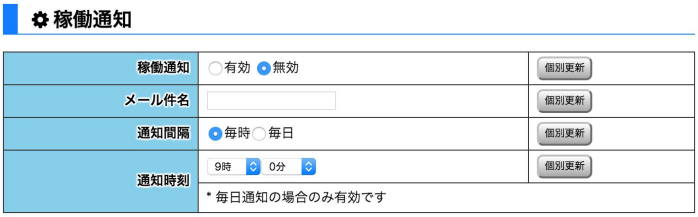
5-4-3. コンピュータ名変化

検知した端末が使っているホスト名が変化した時にメール通知を発行する機能についての設定です。

コンピュータ名変化通知	コンピュータ名変化通知メールを有効/無効化します
メール件名	メールの件名を設定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-4-4. 稼働通知



IntraGuardian本体が動作していることを定期的にメール通知する機能についての設定です。

稼働通知	稼働通知メールを有効/無効化します
メール件名	メールの件名を設定します
通知間隔	メールによる通知間隔を指定します
通知時刻	メールの通知時刻を設定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-4-5. イベント通知

IntraGuardian本体で発生したイベントをメール通知する機能についての設定です。

イベント通知を有効にする	イベント通知メールを有効/無効化します
メール件名	メールの件名を設定します
例外IPアドレスの通知	例外IPアドレスの通知設定を行います

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-5. (監視設定)SNMP設定

5-5-1. SNMPトラップ

SNMPトラップを使って通知をするための設定です。

SNMPトラップ通知	SNMPトラップ通知を有効/無効化します
トラップ送信先	トラップ送信先のアドレスを指定します
コミュニティ名	トラップ送信先のコミュニティ名を入力します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-5-2. 不正接続検知

不正接続を検知した時のSNMPトラップについての設定です。

不正接続検知通知	不正接続検知通知を有効/無効化します
OID	通知のOIDを指定します
可変引数1 タイプ	可変引数1 タイプを指定します
可変引数1 OID	可変引数1 OIDを指定します
可変引数1 値	可変引数1 値を指定します
可変引数2 タイプ	可変引数2 タイプを指定します

可変引数2 OID	可変引数2 OIDを指定します
可変引数2 値	可変引数2 値を指定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-5-3. 不正接続解除

不正端末を登録等により不正接続が解除されたこと時のSNMPトラップについての設定です。

不正接続検知解除通知	不正接続検知解除通知を有効/無効化します
OID	通知のOIDを指定します
可変引数1 タイプ	可変引数1 タイプを指定します
可変引数1 OID	可変引数1 OIDを指定します
可変引数1 値	可変引数1 値を指定します
可変引数2 タイプ	可変引数2 タイプを指定します
可変引数2 OID	可変引数2 OIDを指定します
可変引数2 値	可変引数2 値を指定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-5-4. IPアドレス変化

IPアドレスが変化した時のSNMPトラップについての設定です。

IPアドレス変化通知	IPアドレス変化通知を有効/無効化します
OID	通知のOIDを指定します
可変引数1 タイプ	可変引数1 タイプを指定します
可変引数1 OID	可変引数1 OIDを指定します

可変引数1 値	可変引数1 値を指定します
可変引数2 タイプ	可変引数2 タイプを指定します
可変引数2 OID	可変引数2 OIDを指定します
可変引数2 値	可変引数2 値を指定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-5-5. コンピュータ名変化

コンピュータ名が変化した時のSNMPトラップについての設定です。

コンピュータ名変化通知	コンピュータ名変化通知を有効/無効化します
OID	通知のOIDを指定します
可変引数1 タイプ	可変引数1 タイプを指定します
可変引数1 OID	可変引数1 OIDを指定します
可変引数1 値	可変引数1 値を指定します
可変引数2 タイプ	可変引数2 タイプを指定します
可変引数2 OID	可変引数2 OIDを指定します
可変引数2 値	可変引数2 値を指定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-5-6. 稼働通知

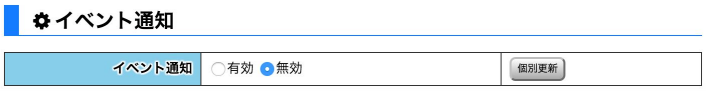
IntraGuardian本体が動作していることを定期的に通知するときのSNMPトラップについての設定です。

稼働通知	稼働通知を有効/無効化します
OID	通知のOIDを指定します
可変引数1 タイプ	可変引数1 タイプを指定します

可変引数1 OID	可変引数1 OIDを指定します
可変引数1 値	可変引数1 値を指定します
可変引数2 タイプ	可変引数2 タイプを指定します
可変引数2 OID	可変引数2 OIDを指定します
可変引数2 値	可変引数2 値を指定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-5-7. イベント通知



IntraGuardian本体で発生したイベントに対するSNMPトラップについての設定です。

イベント通知	イベント通知を有効/無効化します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-6.（監視設定）高度な設定

5-6-1. SYSLOG設定

IntraGuardianが発行するSYSLOGについての設定です。

SYSLOGを利用する	SYSLOGの利用を有効/無効化します
SYSLOGサーバ	SYSLOGサーバのIPアドレスを指定します
ログレベル	ログレベルを指定します

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-7.（監視設定）本体ログイン

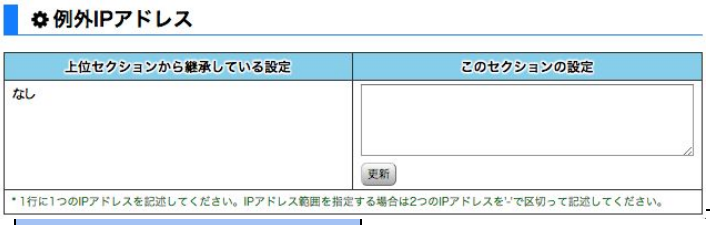
IntraGuardian本体のUIにログインする際のIDとパスワードの設定です。

ログインID	ログインIDを設定します
パスワード	各ログインIDに対応するログインパスワードを設定します
権限	権限を指定します
備考	備考を記入できます

※「本セクションのIntraGuardianの設定を変更する」をクリックすると選択セクションのIntraGuardianの本体設定のみ変更されます。
※「本セクションとその子孫セクションのIntraGuardianの設定を変更する」をクリックすると選択セクションと選択セクション以下の線クションに設定されているIntraGuardianの本体設定が変更されます。
※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-8.（監視設定）例外アドレス

5-8-1. 例外IPアドレス



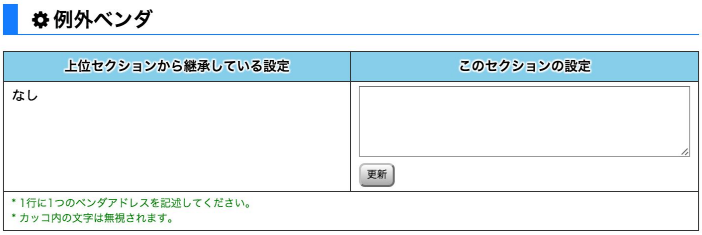
検知／排除の対象としないIPアドレスを設定します。
本項目の設定は、上位のセクションの設定が下位のセクションに継承します。
つまり、「上位セクションから継承している設定」と「このセクションの設定」を合わせたものが IntraGuardian本体に設定されます。

上位セクションから継承している設定	例外IPアドレス一覧が表示されます。 上位セクションで設定された

このセクションの設定	本セクションに設定したい例外IPアドレス一覧を入力します。 1行に1つのIPアドレス、またはIPアドレス範囲を入力してください。

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

5-8-2. 例外ベンダ



検知／排除の対象としないベンダコード（OUIコード）を設定します。
本項目の設定は、上位のセクションの設定が下位のセクションに継承します。
つまり、「上位セクションから継承している設定」と「このセクションの設定」を合わせたものが IntraGuardian本体に設定されます。

上位セクションから継承している設定	上位セクションで設定された例外ベンダー一覧が表示されます。
このセクションの設定	本セクションに設定したい例外ベンダー一覧を入力します。 1行に1つのベンダコード（OUIコード）を入力してください。

※ 設定項目の内容についてはIntraGuardianの本体スタートアップガイドをご参照ください。

6. 端末管理

通常メニューの**端末管理**画面ではIntraGuardian本体で許可する端末を管理することができます。
【3-1. セクションとは】で説明した通り、登録端末は上位のセクションから下位のセクションに継承します。(上位のセクションで登録された端末は、下位のセクションでも登録されているものとして取り扱われます。)

6-1. 端末一覧

端末情報を一覧にて確認できます。

通常は「本セクションで有効な端末」を表示して使いますが、端末を探すなどの際の便宜を図るため、「本セクションに登録されて端末のみ」や「下位セクションのセクションの登録端末を含む」を選択することもできます。

この表示画面からは、右上のボタンを使って次の操作を行うことができます。

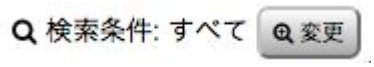
最新の情報にする	ブラウザに最新の情報をリロードします。 **※IntraGuardian本体との同期処理をするわけではありません。**
新規端末登録	新規に端末を登録するページに遷移します。
一括セクション移動	表示されている端末を一括して別のセクションに移動するための子ウィンドウを表示します。
一括削除	表示されている端末を一括削除します。
CSVダウンロード	表示されている端末を一括して、CSVファイルとしてダウンロードします。

6-2. 一覧表示のカスタム

登録端末の一覧表の表示では、表示件数切り替え、ページ切り替え、検索条件指定、表示カラム選択などを行うことができます。この操作は、他の一覧表示でも共通の操作で行うことができます。

なお、検索条件や表示件数などの表示設定内容は、ログインするユーザーごとに保存され、ログアウト後も記憶されます。

6-2-1. 検索条件



検索条件の変更ボタンをクリックすると右図のような検索条件を指定できるウィンドウが表示されます。

ここで、一覧に表示したい条件を指定し適用することで一覧の内容を指定した条件に変更することができます。

この検索条件はログアウト後も保持され、次回ログイン時にも表示されます。

6-2-2. 表示カラム選択

表示カラム選択ボタンをクリックすると、一覧の表示内容をカスタムすることができます。

各項目の表示幅を調整したり、必要の無い項目を非表示にしたり、昇順／降順の変更を行います。

該当列を表示する、表示しないを切り替えることができます。クリックするごとに表示／非表示が切り替わります。

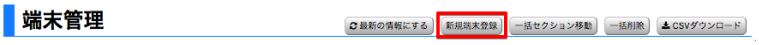
該当列の表示位置を変更します。左から順に、最上位（一覧の一番左）に移動、一つ上（一覧の一つ左）に移動、一つ下（一覧の一つ右）に移動、最下位（一覧の一番右）に移動することができます。

該当行の表示幅を変更します。
この表示幅指定は「**表示する**」になっているすべての幅を100%とした相対指定になります。例えば、表示項目が4つの場合、3つを100%指定、1つを200%指定した場合、1つは他の3つに比べ倍の幅で表示されます。また、3つを50%指定、1つを100%指定した場合も相対指定になるため、前述した1つは他の3つに比べ倍の幅となります。＋記号と－記号はそれぞれ、10%づつ＋と－を行います。

一覧の内容の並び順を変更します。クリックするごとにこの3つのアイコンが切り替わります。
左から、昇順降順の対象としない、昇順指定、降順指定です。
並び順の対象とすることができない項目については、クリックできなくなっています。

6-3. 端末情報の新規登録（新規端末登録）

新しく端末を登録するときは、「新規端末登録」ボタンをクリックします。



すると、**端末管理 － 新規登録**画面に遷移します。

入力する項目は以下の通りです。

登録セクション	これから登録する端末の所属セクションです。
登録セクションの変更	なんらかの理由で、現在着目中のセクション以外のセクションにこの端末を登録したい時に選択します。
端末名	端末につける名前を指定します。 空欄のまま端末を登録すると、自動的に「セクション名+数値」という名前がつけられます。 **※セクション内で重複することはできません。**
端末種別	あらかじめ登録しておいた端末種別を指定できます。（パソコン、プリンタなど）
所有者	この端末の所有者や利用者を入力して、管理しやすくします。
所有者かな	上記所有者のふりがなを入力することが可能です。
有効期限	この端末がネットワークに接続できる期日を入力することが可能です。
IPアドレス変化検知	IPアドレスが変化したことをイベントとして通知するかを選択可能です。
ホスト名変化検知	ホスト名（NetBIOS名かDNS名）が変化したことをイベントとして通知するかを選択可能です。
端末移動検知	端末がセクションを跨がって移動したかどうかをイベントとして通知するかを選択可能です。
資産タグ1	簡易資産管理として利用する場合、お客様で取り決めた情報を入力してください。
資産タグ2	〃
資産タグ3	〃
備考	端末に対する任意のメモ書きです。
ネットワークIF	

MACアドレス	この端末のMACアドレス
NIC種別	あらかじめ登録しておいたネットワークインターフェースの種別を指定できます。(有線、無線など) この情報は検知／排除動作には影響しません。管理をしやすくするための情報です。
登録IPアドレス	この端末が使うべきIPアドレスを登録することができます。

入力完了後、「**新規登録**」ボタンをクリックし登録完了です。

「IPアドレス変化検知」「ホスト名変化検知」「端末移動検知」のデフォルトの値は、**マネージャ設定**画面の**新規端末登録設定**で設定することができます。

「資産管理タグ1」「資産管理タグ2」「資産管理タグ3」は、**マネージャ設定**画面の**UI設定**で表示名称を変更することができます。

登録する端末が複数のNIC(ネットワークインタフェース)を持っている場合は、まず本画面で1つを登録し、次に説明する登録変更画面で残りを追加登録してください。

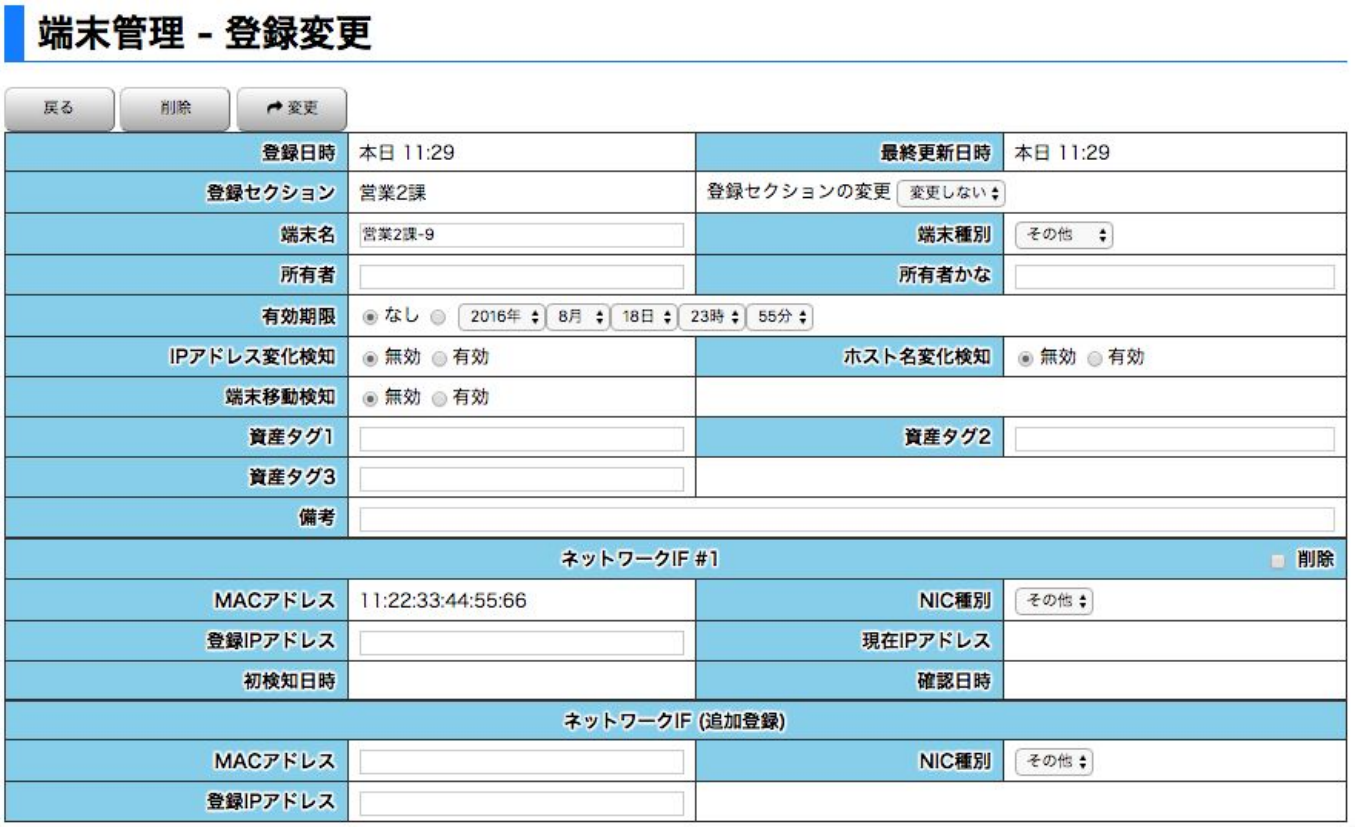
端末のMACアドレスが不明である場合、MACアドレスが空欄のまま登録することも可能です。ただし、IntraGuardian本体で当該端末を識別する術がないため、IntraGuardian本体では登録端末として取り扱われません。

6-4. 端末情報の変更

登録済みの端末情報を編集する場合には、一覧表の1行をクリックします。

登録セクション	端末名	端末種別	有効期限	ホスト名 ワークグループ	初検知日時 確認日時	MACアドレス ベンダ	現在IPアドレス 登録IPアドレス
営業2課	営業2課-1	Windows				00:04:AC:5F:07:61 IBM	
営業2課	営業2課-2	その他				00:04:AC:5F:07:62 IBM	
営業2課	営業2課-3	Linux				00:04:AC:5F:07:63 IBM	
営業2課	営業2課-4	Linux				00:04:AC:5F:07:64 IBM	
営業2課	営業2課-5	Mac				00:04:AC:5F:07:65 IBM	
営業2課	営業2課-6	Printer				00:04:AC:5F:07:66 IBM	
営業2課	営業2課-7	Linux				00:04:AC:5F:07:67 IBM	
営業2課	営業2課-8	Linux				00:04:AC:5F:07:68 IBM	
営業2課	営業2課-9	その他				11:22:33:44:55:66 Unknown	
営業本部	営業本部-1	Linux				3C:D9:2B:8A:11:EB Hewlett Packard	

すると、次のような登録変更画面が表示されます。



端末管理 - 登録変更

戻る　削除　変更

登録日時	本日 11:29	最終更新日時	本日 11:29
登録セクション	営業2課	登録セクションの変更	変更しない
端末名	営業2課-9	端末種別	その他
所有者		所有者かな	
有効期限	なし　2016年 8月 18日 23時 55分		
IPアドレス変化検知	無効 有効	ホスト名変化検知	無効 有効
端末移動検知	無効 有効		
資産タグ1		資産タグ2	
資産タグ3			
備考			
ネットワークIF #1			削除
MACアドレス	11:22:33:44:55:66	NIC種別	その他
登録IPアドレス		現在IPアドレス	
初検知日時		確認日時	
ネットワークIF (追加登録)			
MACアドレス		NIC種別	その他
登録IPアドレス			

変更内容は端末の新規登録時と同じになります。
変更後、「**更新**」ボタンをクリックし変更完了です。

6-5. 端末情報の削除

登録済みの端末情報を削除する場合にも、一覧表の1行をクリックします。

登録セクション	端末名	端末種別	有効期限	ホスト名 ワークグループ	初検知日時 確認日時	MACアドレス ベンダ	現在IPアドレス 登録IPアドレス
営業2課	営業2課-1	Windows				00:04:AC:5F:07:61 IBM	
営業2課	営業2課-2	その他				00:04:AC:5F:07:62 IBM	
営業2課	営業2課-3	Linux				00:04:AC:5F:07:63 IBM	
営業2課	営業2課-4	Linux				00:04:AC:5F:07:64 IBM	
営業2課	営業2課-5	Mac				00:04:AC:5F:07:65 IBM	
営業2課	営業2課-6	Printer				00:04:AC:5F:07:66 IBM	
営業2課	営業2課-7	Linux				00:04:AC:5F:07:67 IBM	
営業2課	営業2課-8	Linux				00:04:AC:5F:07:68 IBM	
営業2課	営業2課-9	その他				11:22:33:44:55:66 Unknown	
営業本部	営業本部-1	Linux				3C:D9:2B:8A:11:EB Hewlett Packard	

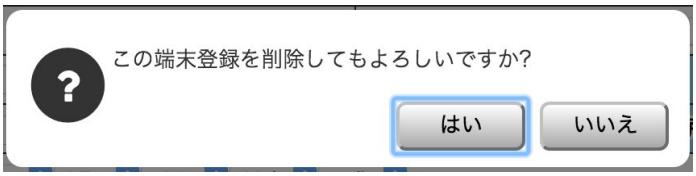
端末管理 - 登録変更

戻る　削除　変更

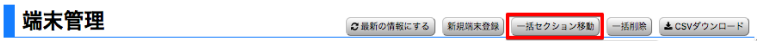
登録日時	本日 11:29	最終更新日時	本日 11:29
登録セクション	営業2課	登録セクションの変更	変更しない
端末名	営業2課-9	端末種別	その他
所有者		所有者かな	
有効期限	なし 2016年 8月 18日 23時 55分		
IPアドレス変化検知	無効 有効	ホスト名変化検知	無効 有効
端末移動検知	無効 有効		
資産タグ1		資産タグ2	
資産タグ3			
備考			
ネットワークIF #1			削除
MACアドレス	11:22:33:44:55:66	NIC種別	その他
登録IPアドレス		現在IPアドレス	
初検知日時		確認日時	
ネットワークIF (追加登録)			
MACアドレス		NIC種別	その他
登録IPアドレス			

登録変更画面が表示されますので、「**削除**」ボタンをクリックしてください。

確認ダイアログが表示されますので、「**はい**」をクリックし削除完了です。



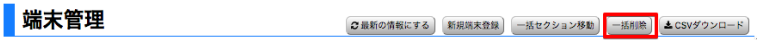
6-6. 一括セクション移動



検索条件に合致するすべての端末を一括して他のセクションに移動することができます。

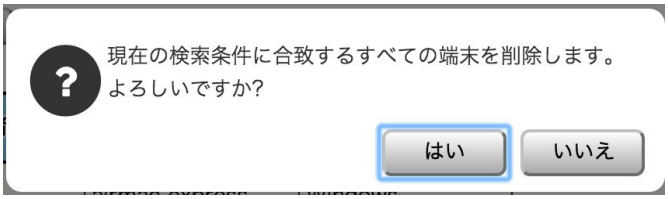
「**一括セクション移動**」ボタンをクリックすると、右図のウィンドウが現れますので、移動先セクションを選択してから「**実行**」ボタンをクリックしてください。

6-7. 端末情報の一括削除



検索条件に合致するすべての端末を一括削除することができます。

「**一括削除**」ボタンをクリックすると、確認画面が表示されますので、「**はい**」をクリックすると削除が完了します。



7. 不正接続一覧

通常メニューの**不正接続一覧**画面では、設置されているIntraGuardianが検知している不正接続端末が表示されます。

この表示画面からは、右上のボタンを使って次の操作を行うことができます。

最新の情報にする	ブラウザに最新の情報をリロードします。 **※IntraGuardian本体との同期処理をするわけではありません。**
一括登録	表示されている端末を一括して登録します。
CSVダウンロード	表示されている端末を一括して、CSVファイルとしてダウンロードします。

7-1. 不正接続一覧からの端末新規登録

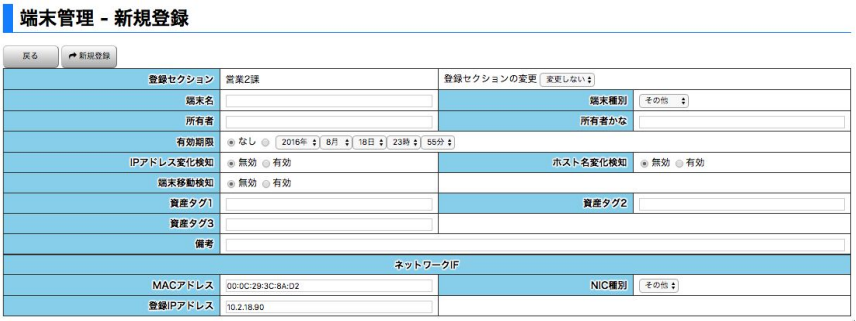
一覧表上の端末をクリックすると、その端末にどのような処理を行うか選択する画面が表示されます。

保留（不正として検出はしているが、排除は行わない）する時間を更新するか、当該端末を正規の端末として登録するかが選択できます。「**端末登録画面へ**」ボタンをクリックすれば、新規登録の画面に遷移します。

※ 保留モードで動作しているIntraGuardianが無い場合は、上記処理選択画面は表示されずに、直接新規登録画面が表示されます。

新規登録の画面は【9-1. 新規端末登録】と同じです。

ただし、「MACアドレス」と「登録IPアドレス」欄は、検知したアドレスで入力済みの状態になっています。



登録が終わると、不正接続一覧画面上では取り消し線表示となります。次にIntraGuardianと通信を行って登録されたことが確認されると、不正接続一覧画面から表示が消えます。

セクション	MACアドレス ベンダ	IPアドレス 別IPアドレス	ホスト名 ワークグループ	OS名 OS種別	検知日時 確認日時	保留時間	状態
~~B1F~~	~~C8:1E:E7:45:41:EA~~ ~~Apple~~	~~192.168.20.157~~ ~~fe80::8d4:5554:e020:3c27~~		~~Mac OS X~~	~~本日 17:35~~ ~~本日 17:35~~	~~0~~	~~検知中~~

7-2. 保留時間の延長

保留時間を延長する場合は、「**端末登録画面へ**」ボタンをクリックせず、直接分数をキーボードから入力するか、「**0**」,「**+30分**」,「**+60分**」,「**+180分**」ボタンをクリックしてから、「**変更**」ボタンをクリックしてください。

入力値は「今から何分間排除を保留するか」という時間であることにご注意ください。

なお、IntraGuardianとの通信によるタイムラグがあるため、1-2分程度の誤差が発生することがあります。

※ 保留モードで動作しているIntraGuardianが無い場合は、上記処理選択画面は表示されませんので、保留時間延長操作はできません。

8. 特別許可端末

特別許可端末では端末登録以外で特別に許可されている端末の状況を表示します。本画面で表示されるのは以下のとおりです。
・「例外IPアドレス」による許可された端末
・「例外ベンダ」による許可された端末
・「外部端末認証」による許可された端末
・「Account@Adapter+連携」による許可された端末

8-1. 特別許可端末からの端末登録

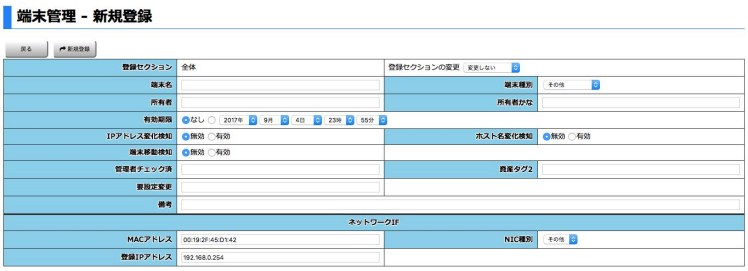
特別許可された端末は、下図のように一覧で表示されます。

登録セクション	MACアドレス ベンダ	検知セクション	現在IPアドレス	ホスト名 ワークグループ	OS名 OS種別	初検知日時 確認日時	登録理由
3F	00:19:2F:45:D1:42 Cisco Systems	3F	192.168.0.254		Windows	本日 16:06 本日 16:19	例外アドレス
2F	00:19:2F:45:D1:43 Cisco Systems	2F	192.168.1.254 fe80::219:2fff:fe45:d143		Windows	本日 16:06 本日 16:19	例外アドレス

一覧から端末登録を行うには、該当の端末を選択します。

上記「端末登録画面へ」ボタンを押下します。

新規登録の画面は【新規端末登録】と同じです。ただし、「MACアドレス」と「登録IPアドレス」欄は、検知したアドレスで入力済みの状態になっています。



8-2. 特別許可端末の端末削除

特別許可された端末は、下図のように一覧で表示されます。

登録セクション	MACアドレス ベンダ	検知セクション	現在IPアドレス	ホスト名 ワークグループ	OS名 OS種別	初検知日時 確認日時	登録理由
3F	00:19:2F:45:D1:42 Cisco Systems	3F	192.168.0.254		Windows	本日 16:06 本日 16:19	例外アドレス
2F	00:19:2F:45:D1:43 Cisco Systems	2F	192.168.1.254 fe80::219:2fff:fe45:d143		Windows	本日 16:06 本日 16:19	例外アドレス

一覧から許可端末削除を行うには、該当の端末を選択します。

上記「特別許可端末を削除」ボタンを押下し、削除します。

9. 履歴

本ソフトウェアで取り扱う履歴には、**端末履歴**と**動作履歴**があります。**端末履歴**は端末に関係する事象の履歴で、**動作履歴**は本ソフトウェアの自動動作やオペレータによる操作の履歴、IntraGuardianの死活状態変化の履歴などです。
通常の運用では、端末履歴のみに注目しておけばよいでしょう。

9-1. 端末履歴

通常メニューの**端末履歴**画面は、端末に対して発生したイベントをセクションごとに表示します。

端末に対するイベントには、次の種類があります。

< 端末イベント一覧 >

不正端末検知	不正端末を検知した
不正端末検知(保留)	不正端末を検知し保留状態にした(一定時間排除を猶予した)
不正端末排除	不正端末を検知し排除を開始した
不正端末情報取得	不正端末情報を取得した
保留時間終了	保留時間が終了した
不正端末追跡終了	不正端末が追跡時間を終了した(ネットワークからいなくなった)
登録端末検出	登録端末がネットワーク内に確認された
許可端末検出	インスペクションによる許可された端末がネットワーク内に確認された
例外IP端末検出	例外IPに登録されているIPアドレスで検知された
例外ベンダ端末検出	例外ベンダで登録されているMACアドレスが検知された
登録端末情報取得	登録端末情報を取得した
登録端末追跡終了	登録端末がネットワーク内からいなくなったり指定された追跡時間が経過した
有効期限切れ	登録端末で有効期限が切れている端末をネットワーク内に検知した

登録IPアドレス違反	IPアドレス監視が有効になっている登録端末が登録IPアドレスと異なるIPアドレスを利用していることを検知した
コンピュータ名変化	登録端末でコンピュータ名が変化した
IPアドレス変化	登録端末でIPアドレスが変化した
端末移動	セクション間で登録端末が移動した
保留時間変更	不正端末の保留時間を変更した
端末登録申請	利用申請機能により登録申請が行われた
登録申請却下	利用申請昨日の登録申請を却下した

9-2. 動作履歴

マネージャメニューの動作履歴画面では、本ソフトウェアの自動動作やオペレータによる操作の履歴、IntraGuardianの死活状態変化の履歴などを表示します。

※ 動作履歴は、全権管理者の権限を持ったオペレータしか確認することはできません。

日時	分類	重要度	オペレータ	内容
2016/08/18 09:35:04	IG関連	通常動作	SYSTEM	営業2課-東京の登録端末を同期しました
2016/08/18 09:34:57	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業2課-東京:10.2.22.1)
2016/08/18 09:34:57	IG関連	通常動作	SYSTEM	IntraGuardianのマネージャ通信が切断しました(営業2課-東京:10.2.22.1)
2016/08/18 09:34:53	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業2課-東京:10.2.22.1)
2016/08/18 09:34:43	IG関連	通常動作	SYSTEM	営業2課-札幌の登録端末を同期しました
2016/08/18 09:34:39	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業2課-札幌:10.2.20.1)
2016/08/18 08:55:48	オペレータ関連	通常動作	スーパーユーザ	admin is logged in.
2016/08/18 08:24:04	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業2課:10.2.18.1)
2016/08/18 08:23:57	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(開発部:10.2.21.1)
2016/08/17 20:01:16	IG関連	通常動作	SYSTEM	IntraGuardianのマネージャ通信が切断しました(開発部:10.2.21.1)
2016/08/17 20:01:16	IG関連	通常動作	SYSTEM	IntraGuardianのマネージャ通信が切断しました(営業2課:10.2.18.1)
2016/08/17 17:15:41	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(開発部:10.2.21.1)
2016/08/17 17:15:41	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業2課:10.2.18.1)
2016/08/17 17:15:31	その他	通常動作	SYSTEM	Start IntraGuardian2+ Manager Professional on /Users/shibuya/work/NCAD/IntraGuardian/ig2mla/src/IG2MLA
2016/08/17 17:15:29	その他	通常動作	SYSTEM	Stop IntraGuardian2+ Manager Professional on /Users/shibuya/work/NCAD/IntraGuardian/ig2mla/src/IG2MLA
2016/08/17 16:04:24	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業2課:10.2.18.1)
2016/08/17 16:04:22	IG関連	通常動作	SYSTEM	営業2課の登録端末を同期しました
2016/08/17 13:54:37	セクション関連	重要動作	スーパーユーザ	Delete section 開発部 from parents of 営業3課
2016/08/17 13:50:05	セクション関連	重要動作	スーパーユーザ	Add section 開発部 as a parent of 営業3課
2016/08/17 13:23:40	セクション関連	重要動作	スーパーユーザ	Delete section 開発部 from parents of 営業3課
2016/08/17 13:19:54	セクション関連	重要動作	スーパーユーザ	Add section 開発部 as a parent of 営業3課
2016/08/17 13:19:47	セクション関連	重要動作	スーパーユーザ	Delete section 開発部 from parents of 営業2課
2016/08/17 13:19:32	セクション関連	重要動作	スーパーユーザ	Add section 開発部 as a parent of 営業2課
2016/08/17 10:40:34	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業2課:10.2.22.1)
2016/08/17 10:36:55	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(開発部:10.2.21.1)
2016/08/17 10:35:16	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業2課-東京:10.2.20.1)
2016/08/17 10:09:18	IG関連	通常動作	SYSTEM	IntraGuardianがマネージャと通信開始しました(営業1課:10.2.18.1)
2016/08/17 10:09:15	IG関連	通常動作	SYSTEM	営業1課の登録端末を同期しました
2016/08/17 09:50:28	セクション関連	重要動作	スーパーユーザ	Add '開発部'(33732113) as a child section of '全体'
2016/08/17 09:30:48	その他	通常動作	SYSTEM	Start IntraGuardian2+ Manager Professional on /Users/shibuya/work/NCAD/IntraGuardian/ig2mla/src/IG2MLA
2016/08/17 09:30:45	その他	通常動作	SYSTEM	Stop IntraGuardian2+ Manager Professional on /Users/shibuya/work/NCAD/IntraGuardian/ig2mla/src/IG2MLA

前ページ　次ページ

記録される履歴は4つに分類され保存されています。検索条件を使ってこれらを絞り込んで表示することもできます。

IG関連	IntraGuardianの管理について発生したイベント
オペレータ関連	オペレータの重要な操作（ログインなど）

セクション関連	セクションの追加や削除など
その他	上記のいずれにも属さない事象

IntraGuardian関連のイベントには以下の種類があります。

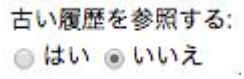
＜IG関連イベント一覧＞

リンクアップ	IntraGuardianがリンクアップした
エンジン再起動	IntraGuardianの検知・排除システムが再起動した
エンジン停止	IntraGuardianの検知・排除システムが停止した
マネージャ接続開始	IntraGuardianが本ソフトウェアと接続開始した
マネージャ接続切断	IntraGuaridnaが本ソフトウェアとの接続を終了した
例外ベンダ登録	例外ベンダが新規登録された
例外ベンダ削除	例外ベンダが削除された
例外IP登録	例外IPが新規登録された
例外IP削除	例外IPが削除された
登録端末一覧リストア	登録端末情報が復元された
登録端末一覧同期	登録端末情報が本ソフトウェアと同期された

9-3. 新しい履歴と古い履歴

端末履歴、動作履歴は、多数のレコードが蓄積されてゆくため、表示や検索を快適に行えるように「最近の履歴」と「古い履歴」に分けて保存されています。「最近の履歴」は、過去31日以内のものを指し、「古い履歴」はそれ以前のものを指します。

端末履歴画面、動作履歴画面には、右側に古い履歴を参照するかどうかを選択するラジオボタンがついています（右図）。



「いいえ」を選択しておくと、新しい履歴のみを表示／検索対象とするため、素早く動作致します。

また、端末履歴、動作履歴共に、366日より昔のものは自動的に削除されてゆきます。この履歴の整理作業は、1日に1回深夜に実行されます。

上に述べた、最近の履歴とする日数、履歴の保存期間、履歴整理の時刻については、マネージャ設定画面の「履歴設定」で変更することができます。お使いの環境に合わせて調整をしてください。

10. マネージャ設定

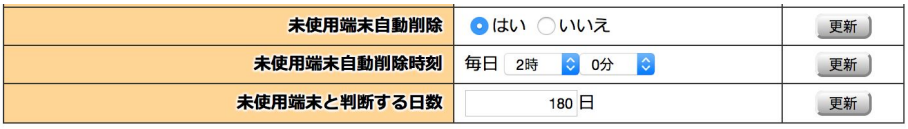
マネージャ設定画面では本ソフトウェア自体の設定を行うことが出来ます。
マネージャ設定は、

- 動作設定
- UI設定
- メール通知設定
- その他通知設定
- バックアップ設定
- 履歴設定
- 新規端末登録設定
- 登録申請設定
- 外部端末認証設定
- Account@Adapter+ 連携設定

の、10項目からなります。

10-1. (マネージャ設定)動作設定

動作設定では、主にIntraGuardianとの通信についての設定を行います。

IGステータス確認間隔	IntraGuardian と通信を行う間隔(ポーリング間隔)を設定します。 環境によって10秒～180秒程度で設定してください。
検知情報収集間隔	IntraGuardian が不正接続として認識した端末の情報や、現在ネットワークに接続されている端末の情報を収集する間隔を設定します。 環境によって10秒～180秒程度で設定してください。 **※検知情報収集間隔は設定した以上のIGステータス確認間隔の倍数値で動作致します。 例えば、IGステータス確認間隔を10秒、検知情報収集間隔を15秒と設定していた場合は、 検知情報収集間隔は20秒で実行されることになります。**
登録端末強制同期	IntraGuardian と通信が成立している際には、登録情報に差分が生じた場合は自動的に同期が行われますが、強制的に同期をさせる時刻を指定することができます。 本項目を「はい」にすると「登録端末強制同期時刻」の項目が表示されます。  毎日 ○時○分 という時間指定を入力してください。 **※通常設定する必要はありません。**
端末移動監視	端末がセクションを跨いで移動したかどうかをトラッキングしたい場合に利用します。
未使用端末自動削除	一定時間ネットワーク上に存在を確認できなかった端末を自動的に削除する場合に指定します。 本項目を「はい」にすると「未使用端末自動削除時刻」および「未使用端末と判断する日数」の項目が表示されます。  未使用チェックを行う時間を 毎日 ○時○分で指定し、未使用端末と判断する日数を入力し

	てください。

10-2. (マネージャ設定)UI設定

UI設定では、本ソフトウェアのUI画面上の動作の設定を行います。

ログインタイムアウト	操作が無かった場合、ログアウトさせるまでの時間を設定できます。
資産タグ1表示名称	簡易資産管理を行う場合、登録済み端末に任意の項目を3カ所用意できます。 本欄に入力すると、本ソフトウェアのUI上で「資産タグ1」と表示している部分がすべて入力した文字列に置換されます。
資産タグ2表示名称	〃
資産タグ3表示名称	〃

10-3. (マネージャ設定)メール通知設定

メール通知設定ではメールの送信に関する設定を行うことができます。
また、本設定が適切であるかどうかを確認するためのテストメールを発信することができます。

メール通知機能使用	メール通知機能を利用するかしないかを設定します。
SMTPサーバ	メール送信のためのSMTPサーバを指定します。
SMTPポート番号	SMTPサーバのポート番号を指定します。 通常 25番もしくは 587番です。
SSL利用	SMTPサーバが STARTTLS に対応している場合、「STARTTLS 対応」を選択してください。 SMTPサーバが STARTTLS に対応しているが、正規のサーバ証明書を持っていないという場合には「STARTTLS(証明書無視)」を選択してください。
送信元メールアドレス	メール通知の送信元メールアドレスを指定します。
SMTP認証タイプ	SMTPサーバが認証を行う場合の方式を指定できます。 POP Before SMTP認証の場合には、POPサーバ、POPポート番号、POPアクセス待ち時間、ユーザ名、パスワードを入力してください。 SMTPAUTH認証の場合には、ユーザ名とパスワードを入力してください。
メール集約時間	連続してメール通知が行われないように、イベントが発生してから本項目の時間を待ってから送信できます。その間に発生した他のイベントは、イベントの種類ごとに集約されます。
イベント集約	全てのイベントを一つのメールに集約する場合は「全イベントを集約」を選択してください。 イベントの種類ごとの集約にとどめる場合は「イベントグループごとに集約」を選択してください。
メール送信処理タイムアウト	メール送信にかける最大時間を指定します。メールサーバとの通信時間がこれ以上にになる場合は、送信失敗とみなします。
文字エンコーディング	文字コードのエンコーディングを指定します。 日本語の場合は ISO2022JPもしくはUTF8を選択してください。
文面カスタマイズ	**※詳細は「13-3-1. メールの文面をカスタマイズする」を参照**
テストメール送信	宛先を入力して[送信]ボタンをクリックするとメールが送信されます。 設定が間違っていないかどうかの確認にご利用ください。

10-3-1. メールの文面をカスタマイズする

本ソフトウェアではメールの文面をカスタマイズすることが可能です。カスタマイズにはメール表題と、各イベントを知らせるメール文面の2つの文字列があります。
本文の文字列には変数（本ソフトウェアが自動的に置き換える文字列)を含めることができます。使用できる変数は次の通りです。

- {section} は、セクション名に置き換えられます
- {oldsection} は、以前のセクションに置き換えられます
- {hostname} は、ホスト名に置き換えられます
- {oldhostname} は、以前のホスト名に置き換えられます
- {hostos} は、OS名に置き換えられます
- {hosttype} は、TYPE名に置き換えられます
- {workgroup} は、ワークグループ名に置き換えられます
- {lladdr} は、イベントが発生した際のMACアドレスに置き換えられます
- {ipaddr} は、イベントが発生した際のIPアドレスに置き換えられます
- {orgipaddr} は、登録されているIPアドレスに置き換えられます
- {expiretime} は、有効期限に置き換えられます
- {reservetime} は、保留時間に置き換えられます
- {oldipaddr}は、IPアドレス変化時の変化前IPアドレスに置き換えられます
- {note}は、利用申請時の備考に置き換えられます
- {igipaddr}は、IntraGuardianのIPアドレスに置き換えられます

※表題には変数を含めることはできません。

表題		
共通の表題 （全イベントを集約するとき）		メールの表題（Subject:）になる文面です
不正端末検知系 登録端末検出系 端末変化検出系 端末登録系 IG起動系 例外登録系 一括登録系 （イベントグループごとに集約するとき）		それぞれのイベント種別のメールの表題（Subject:）になる文面です
本文		
不正端末検知系イベントグループ	**不正端末検知**	不正接続端末を検知したときの文面です
	不正端末検知（保留）	不正接続端末を検知し、保留となったときの文面です
	不正端末排除	不正接続端末の排除を開始したときの文面です
	不正端末情報取得	不正接続端末の詳細情報が取得できたときの文面です
	保留時間終了	保留中の不正接続端末の保留時間が終了したときの文面です
	不正端末追跡終了	不正接続端末がネットワーク上から見当たらなくなったときの文面です
	有効期限切れ	登録済み端末の有効期限が切れた場合の文面です
	登録IPアドレス違反	登録済み端末が指定されたIPアドレスを利用していないときの文面です
登録端末検	**登録端末検出**	登録済みの端末がネットワーク上で検出されたときの文面です

出系イベントグループ	許可端末検出	※ 現在本項目は無効です
	例外IP端末検出 例外ベンダ端末検出	例外IPアドレスや、例外ベンダ機能で一時的に登録した場合の文面です
	登録端末情報取得	登録済み端末の詳細情報が取得できたときの文面です
	登録端末追跡終了	登録済み端末がネットワーク上から見当たらなくなったときの文面です
端末変化検出系イベントグループ	コンピュータ名変化	コンピュータ名(NetBIOS名/DNS名)が変化したときの文面です
	IPアドレス変化	利用しているIPアドレスが変化したときの文面です
	端末移動	端末がセクション間で移動したときの文面です
端末登録系イベントグループ	保留時間変更	不正接続端末の保留時間が変更されたときの文面です
	端末登録申請	不正接続端末から利用申請が送られたときの文面です
IG起動系イベントグループ	電源ON	IntraGuardian の電源がONになったときの文面です
	リンクダウン	IntraGuardian のLANポートがリンクダウンしたときの文面です ※リンクダウン中はイベントを送れないので、かなり遅延して発生します。
	リンクアップ	IntraGuardian のLANポートがリンクアップしたときの文面です
	エンジン再起動	IntraGuardian のソフトウェアが再起動したときの文面です ※本メールが頻発する際は、ユーザーサポートまでご連絡ください。
	エンジン停止	IntraGuardian のソフトウェアが停止したときの文面です ファームウェアアップデートの際に発生する可能性があります
	マネージャ接続開始	IntraGuardian が本ソフトウェアと通信を開始した際の文面です
	マネージャ接続切断	IntraGuardian が本ソフトウェアと切断した際の文面です
例外登録系イベントグループ	例外ベンダ登録	例外ベンダが登録された際の文面です
	例外ベンダ削除	例外ベンダが削除された際の文面です
	例外IP登録	例外IPアドレスが登録された際の文面です
	例外IP削除	例外IPアドレスが削除された際の文面です
一括登録系イベントグループ	登録端末一覧リストア	登録済み端末一覧がファイルからリストアされた際の文面です
	登録端末一覧同期	IntraGuardian との同期処理が行われた際の文面です

10-4.（マネージャ設定）その他通知設定

10-4-1. SYSLOG設定

本ソフトウェアからSYSLOGに出力することができます。通知内容は、メール通知のイベントと同様に設定ができます。

SYSLOGサーバ	SYSLOGサーバのアドレスを指定します
出力レベル	SYSLOG出力のログレベルを指定します
ファシリティ	SYSLOGのファシリティを指定します
イベントごとの詳細設定	各イベントごとにログレベルを変更できます
テスト送信	SYSLOGへテスト出力します

10-4-2.SNMPトラップ設定

本ソフトウェアからSNMPトラップ通知の設定を行えます。通知内容は、メール通知のイベントと同様に設定ができます。

SNMPトラップ通知使用	SNMPトラップ通知を行うか指定します
SNMPトラップ先	SNMPトラップ先を指定します
SNMPコミュニティ名	SNMPのコミュニティを指定します
イベントごとの詳細設定	各イベントごとにSNMPトラップの発行を行うかの指定とOIDを指定できます
テスト送信	SNMPトラップのテスト通知を行います テスト用のSNMPトラップは次のOIDで送られます: .1.3.6.1.4.1.26898.3.2.9999

10-5.（マネージャ設定）バックアップ設定

10-5-1. ファイル保存方式の自動バックアップ

自動バックアップの設定内容は、「**メンテナンス**」の「**バックアップ復元**」と同じになります。

※ メンテナンスと別の設定を入れることはできません。

1. 自動バックアップを「はい」を選択し右側の「**更新**」ボタンをクリック
2. 自動バックアップ時刻を選択し右側の「**更新**」ボタンをクリック
3. バックアップ先を「**ファイル保存**」を選択し右側の「**更新**」ボタンをクリック
4. バックアップ内容を選択（**※前述確認**）し右側の「**更新**」ボタンをクリック
5. バックアップファイルを暗号化するためのキーを入力し右側の「**更新**」ボタンをクリック
6. ディレクトリへ保存先ディレクトリを**フルパス**（**絶対パス**）で指定し右側の「**更新**」ボタンをクリック

上記でファイル保存の自動バックアップ設定完了です。

10-5-2. FTP保存方式の自動バックアップ

自動バックアップの設定内容は、「**メンテナンス**」の「**バックアップ復元**」と同じになります。

※ メンテナンスと別の設定を入れることはできません。

1. 自動バックアップを「はい」を選択し右側の「**更新**」ボタンをクリック
2. 自動バックアップ時刻を選択し右側の「**更新**」ボタンをクリック
3. バックアップ先を「**FTP保存**」を選択し右側の「**更新**」ボタンをクリック
4. **FTPサーバ**のアドレスを入力し右側の「**更新**」ボタンをクリック　**※ホスト名指定をする場合はセットアップPCからの名前解決をご確認の上ご利用ください**
5. **FTPユーザ**、**FTPパスワード**を入力し右側の「**更新**」ボタンをクリック
6. **FTPディレクトリ**を入力し右側の「**更新**」ボタンをクリック
7. **FTPモード**を「**パッシブ**（**アクティブ**）」を選択し右側の「**更新**」ボタンをクリック

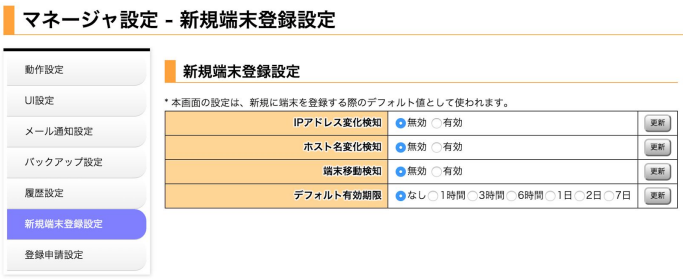
10-6.（マネージャ設定）履歴設定

履歴設定では、動作履歴と端末履歴の取り扱いに関する設定をします。
各項目の詳しい内容については【8-3. 新しい履歴と古い履歴】を参照してください。
※本画面は、クラウド版マネージャをご利用の場合は操作できません。

動作履歴保存期間	動作履歴の保存期間を指定します
端末履歴保存期間	端末履歴の保存期間を指定します
最近の履歴とする日数	「最近の履歴」とする日付を指定します
履歴整理時刻	保存期間を超えた履歴を削除する処理を実行する時刻を指定します。 **※できるだけサーバの負荷の少ない時刻を指定することをおすすめします**
履歴整理	履歴整理を直ちに行います

10-7.（マネージャ設定）新規端末登録設定

新規端末登録画面のデフォルト値を設定できます。



IPアドレス変換検知	IPアドレス変化検知の初期値を設定可能です
ホスト名変化検知	ホスト名変化検知の初期値を設定可能です
端末移動検知	端末移動検知の初期値を設定可能です
デフォルト有効期限	あらかじめ入力される有効期限の値を設定可能です

10-8.（マネージャ設定）登録申請設定

登録申請設定では、登録申請機能に関する設定をします。
詳細は【13. 登録申請機能】をご覧ください。
※本機能はクラウド版マネージャをご利用の場合は操作できません。
※本機能はAccount@Adapter+連携が有効の場合は操作できません。

10-9.（マネージャ設定）外部端末認証設定

外部端末認証設定では、Radiusサーバを利用し本ソフトウェア以外で認証された端末の通信を許可する仕組みです。

※外部端末認証により許可されていない端末でも、端末登録で登録されている端末は許可されますのでご注意ください。

※本機能はAccount@Adapter+連携設定と同時に使用することはできません。

外部端末認証	Radius認証を利用するかどうかを指定します **※Account@Adapter+連携と同時に利用できません**
外部認証サーバ	Radius認証をする認証サーバアドレスを指定します
外部認証サーバ(Slave)	Radius認証をする認証サーバ（冗長化の場合の）アドレスを指定します
外部認証方式	認証方式（CHAP または PAP）を指定します
外部認証共有鍵	PAPの場合の認証共有鍵を指定します
外部認証NAME属性値	認証時のNAME属性内容を指定します
外部認証PASSWORD値	認証時のPASSWORD値の内容を指定します **※空欄の場合はMAcアドレスが送られます**
外部認証応答待ち時間	認証サーバの認証応答待ち時間（**ミリ秒**）を指定します
外部認証リトライ回数	認証サーバの認証リトライ回数を指定します
外部認証切り戻し時間	認証サーバのSlaveからMasterへのkりい代わり時間（**分**）を指定します
登録セクション	認証成功時の登録されるセクションを指定します
登録再認証時間	登録端末の再認証時間（**秒**）を指定します
不正端末再認証時間	不正端末の再認証時間（**秒**）を指定します

10-10.（マネージャ設定）Account@Adapter+ 連携設定

Account@Adapter+ 連携設定では、Account@Adapter+で認証許可された端末の通信を許可する仕組みです。
※Account@Adapter+により許可されていない端末でも、端末登録で登録されている端末は許可されますのでご注意ください。
※本機能は外部端末認証設定と同時に使用することはできません。
※本機能は登録申請機能と同時に使用することはできません。

Account@Adapter+連携	Radius認証を利用するかどうかを指定します **※外部端末認証設定と同時に利用できません**
登録申請WEBサーバ	Account@Adapter+サーバアドレスを指定します
登録申請URLプレフィックス	Account@Adapter+の申請機能のURLを指定します **※設定によりURLが異なりますのでAccount@Adapter+の設定に合わせて変更してください**
登録申請WEB接続待ち時間	登録申請WEBサーバへの接続待ち時間を指定します **※問題がない場合以外デフォルト値をご利用ください**
登録申請WEBリトライ回数	**※現在未使用項目です**
登録申請WEB切り戻し時間	**※現在未使用項目です**
外部認証サーバ	Account@Adapter+サーバアドレスを指定します
外部認証サーバ(Slave)	Account@Adapter+サーバ（冗長化の場合の）アドレスを指定します
外部認証方式	認証方式（CHAP または PAP）を指定します
外部認証共有鍵	PAPの場合の認証共有鍵を指定します
外部認証PASSWORD値	認証時のPASSWORD値の内容を指定します **※空欄の場合はMAcアドレスが送られます**
外部認証応答待ち時間	認証サーバの認証応答待ち時間（**ミリ秒**）を指定します
外部認証リトライ回数	認証サーバの認証リトライ回数を指定します
外部認証切り戻し時間	認証サーバのSlaveからMasterへのkりい代わり時間（**分**）を指定します
登録セクション	認証成功時の登録されるセクションを指定します
登録再認証時間	登録端末の再認証時間（**秒**）を指定します
不正端末再認証時間	不正端末の再認証時間（**秒**）を指定します

11. 管理者・オペレータの設定

11-1. 権限

本ソフトウェアでは以下の4種類の権限を持ったオペレータ(操作者)を作成することができます。

閲覧者	特定セクションの登録端末や不正端末、設定状態の閲覧ができます。
管理者	閲覧者の権限に加え、特定セクションの登録端末や不正端末の登録内容変更ができます。
システム管理者	管理者の権限の加え、特定セクションの設定の変更と、特定セクションの閲覧者・管理者・システム管理者の変更ができます。
全権管理者	すべての操作ができます。

オペレータは任意の人数登録することができます。
インストール直後は、全権管理者が1名のみ登録されています。

11-2. オペレータ設定

オペレータの一覧は、マネージャメニューのオペレータ設定画面で表示できます。

※ オペレータ情報は全権管理者の権限を持ったオペレータのみ操作可能です。

オペレータ設定の一覧には現在存在している**オペレータ**が表示されます。使用開始直後は、セットアップ時に指定したオペレータが表示されています。

11-2-1. オペレータの新規登録

オペレータ設定の「**新規登録**」ボタンをクリックし新規登録画面を表示します。

オペレータ設定

オペレータの情報として以下の項目を入力します。(※は必須入力項目です。)

< 設定項目一覧 >

名称※	オペレータの**表示名**を指定します
ログインID※	ログイン時に使用する**ID**を指定します。すでに登録しているオペレータと同じIDを指定することはできません。
パスワード※ (パスワード確認用)	ログイン時に使用する**Password**を指定します(確認用には同じものを入力します)
メールアドレス	メール通知使用時に通知する**メールアドレス**を指定します
連絡先	オペレータの**連絡先**を指定します **※ 登録申請画面に表示される文字列です。任意文字列を指定できます。**
言語	オペレータが使用する**言語**を指定します。現在は**日本語**固定です。
タイムゾーン	オペレータが使用する**タイムゾーン**を指定します
アクセス権限	オペレータの**アクセス権限**を指定します **※各権限の違いは本章の先頭を参照してください。**
備考	オペレータについての**情報**を記載します **※ソフトウェアでは利用しません。管理上任意に指定可能なフィールドになります。**
メール通知	
不正端末検知	管理しているセクションで不正端末を検知した際に通知するかどうかを指定します
不正端末検知(保留)	管理しているセクションで不正端末を検知し保留した際に通知するかどうかを指定します
不正端末排除	管理しているセクションで不正端末を検知し排除した際に通知するかどうかを指定します

不正端末情報取得	管理しているセクションで不正端末情報を取得した際に通知するかどうかを指定します
保留時間終了	管理しているセクションで保留時間が終了した端末を通知するかどうかを指定します
不正端末追跡終了	管理しているセクションで不正端末が追跡時間を終了した（ネットワークからいなくなった）際に通知するかどうかを指定します
登録端末検出	管理しているセクションで登録端末がネットワーク内に確認された際に通知するかどうかを指定します
許可端末検出	管理しているセクションでインスペクションによる許可された端末がネットワーク内に確認された際に通知するかどうかを指定します
例外IP端末検出	管理しているセクションで例外IPに登録されているIPアドレスで検知された際に通知するかどうかを指定します
例外ベンダ端末検出	管理しているセクションで例外ベンダで登録されているMACアドレスが検知された際に通知するかどうかを指定します
登録端末情報取得	管理しているセクションで登録端末情報を取得した際に通知するかどうかを指定します
登録端末追跡終了	管理しているセクションで登録端末がネットワーク内からいなくなったり指定された追跡時間が経過した際に通知するかどうかを指定します
有効期限切れ	管理しているセクションで登録端末で有効期限が切れている端末をネットワーク内に検知した際に通知するかどうかを指定します
登録IPアドレス違反	管理しているセクションでIPアドレス監視が有効になっている登録端末が登録IPアドレスと異なるIPアドレスを利用していることを検知した際に通知するかどうかを指定します
コンピュータ名変化	管理しているセクションで登録端末でコンピュータ名が変化した際に通知するかどうかを指定します
IPアドレス変化	管理しているセクションで登録端末でIPアドレスが変化した際に通知するかどうかを指定します
端末移動	管理しているセクション間で登録端末が移動した場合に通知するかどうかを指定します
リンクアップ	管理しているセクションでIntraGuardianがリンクアップした際に通知するかどうかを指定します
エンジン再起動	管理しているセクションでIntraGuardianの検知・排除システムが再起動した際に通知するかどうかを指定します
エンジン停止	管理しているセクションでIntraGuardianの検知・排除システムが停止した際に通知するかどうかを指定します
マネージャ接続開始	管理しているセクションでIntraGuardianが本ソフトウェアと接続開始した際に通知するかどうかを指定します
マネージャ接続切断	管理しているセクションでIntraGuaridnaが本ソフトウェアとの接続を終了した際に通知するかどうかを指定します
例外ベンダ登録	管理しているセクションで例外ベンダが新規登録された際に通知するかどうかを指定します
例外ベンダ削除	管理しているセクションで例外ベンダが削除された際に通知するかどうかを指定します
例外IP登録	管理しているセクションで例外IPが新規登録された際に通知するかどうかを指定します
例外IP削除	管理しているセクションで例外IPが削除された際に通知するかどうかを指定します
登録端末一覧リストア	管理しているセクションで登録端末情報が復元された際に通知するかどうかを指定します
登録端末一覧同期	管理しているセクションで登録端末情報が本ソフトウェアと同期された際に通知するかどうかを指定します

最後に「**新規登録**」ボタンをクリックし登録完了です。

11-2-2. オペレータ情報の変更

オペレータ情報の変更をする場合は、変更するオペレータの右側にある「**編集**」ボタンをクリックします。項目は新規登録と同じです。

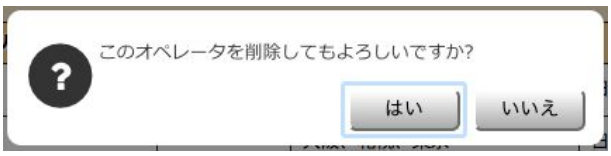
※パスワードを変更しない場合は空欄にしてください。

変更後、「**更新**」ボタンをクリックすると変更完了です。

11-2-3. オペレータの削除

オペレータの削除は、削除したいオペレータの右側にある「**削除**」ボタンをクリックします。

確認ダイアログが表示されるので、「**はい**」を選択します。



上記にて削除完了です。

※ 現在操作をしている自分自身を削除することはできません。

11-3. 自分の情報（個人情報）を変更する

オペレータの新規作成や自分以外のオペレータ情報の変更は**全権管理者**の権限を持ったオペレータしか操作することはできませんが、全権管理者以外のオペレータは自分の情報のみ変更可能です。変更方法は以下の通りです。

トップメニューの「**個人情報**」をクリックし個人情報画面を表示します。

変更後、「**更新**」ボタンをクリックし変更完了です。

※ 個人情報画面はオペレータの変更と内容はほぼ同じですが、変更を適用するためには現パスワードを入力する必要があります。

11-4. セクションの管理権限

11-4-1. セクションの管理権限付与

全権管理者以外のオペレータは、作成直後はどのセクションにも管理権限を持たないため、何もすることができません。
各オペレータが管理することができるセクションを設定しましょう。

※ 全権管理者は初めから全セクションに対してすべての操作をすることができるため、本節の作業をする必要がありません。

まず、**通常メニュー**の**セクション管理**画面を表示します。そこで、【3-3. 着目セクションの切り替え】で示した方法で、セクションを選択します。

その後、セクション管理画面の**本セクションの管理者/閲覧者**欄の「**管理者/閲覧者の追加**」ボタンをクリックします。

すると、追加可能なオペレータの一覧が表示されるので、追加するオペレータの行ををクリックします。

これで指定したオペレータはこのセクションを管理（閲覧）することができるようになりました。

なお、セクションの管理権限は、子の方向に継承します。つまり、「営業2課」に権限を持つオペレータは、自動的に「営業2課-東京」と「営業2課-札幌」にも権限を持つことになります。

一人のオペレータが複数のセクションの管理権限を持つこともできます。それぞれのセクションで「管理者／閲覧者の追加」を行ってください。

11-4-2. セクションの管理権限剥奪

セクションに対するオペレータの管理権限を剥奪するのにも、通常メニューのセクション管理画面を用います。

割り当てを削除したいオペレータの「**削除**」ボタンをクリックするだけで、管理権限を剥奪することができます。

※ ここで削除されるのは、このセクションに対する管理権限だけであり、オペレータ自身が削除されるわけではありません。

なお、全権管理者は常に全てのセクションの管理権限を持っていますので、「削除」ボタンは表示されません。また、上位のセクションに権限を持っているために継承して管理権限を持っているオペレータについても、「削除」ボタンは表示されません。

12. 種別管理

マネージャメニューの**種別管理**画面では、端末管理で利用する端末種別とNIC種別を変更することができます。

端末種別、NIC種別ともに、検知や排除の動作にはまったく影響がありません。端末の管理をしやすくするための補助情報です。

12-1. 端末種別

端末種別は、端末の種類を示す名称です。例えば、”Windows”、”MacOS”、”Linux” などのOSの種類名や、”ルータ”、”スイッチ”、”プリンタ”、”スキャナ”などの機器の種類を示す名前を設定することを想定しています。

12-1-1. 端末種別の新規登録

端末種別にある「**新規登録**」ボタンをクリックします。

新しく設定する「**端末種別名**」を入力します。
入力が完了したら、「**新規登録**」ボタンをクリックし完了です。

12-1-2. 端末種別の変更

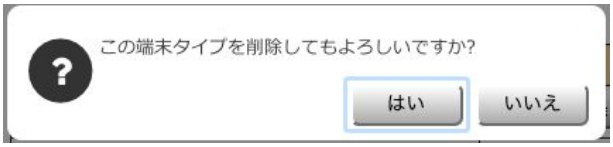
変更したい端末種別の右側にある「**編集**」ボタンをクリックします。

新しい「**端末種別名**」を入力します。
入力が完了したら、「**変更**」ボタンをクリックし完了です。

12-1-3. 端末種別の削除

削除したい端末種別の右側にある「**削除**」ボタンをクリックします。

確認ダイアログが表示されますので、「**はい**」をクリックし削除完了です。



※初期設定で「その他」と設定されている項目は削除することはできません。名称を変更することはできます。

12-2. NIC種別

NIC種別は、NIC（ネットワークインタフェース）ごとの種類を示す名称を設定できます。例えば、「有線」「無線」「USB有線」などを設定できます。

12-2-1. NIC種別の新規登録

NIC種別にある「**新規登録**」ボタンをクリックします。

新しく設定する「**NIC種別名**」を入力します。
入力が完了したら、「**新規登録**」ボタンをクリックし完了です。

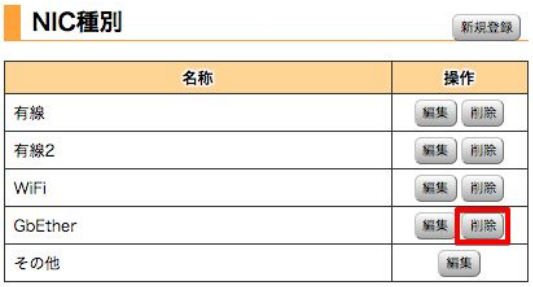
12-2-2. NIC種別の変更

変更したいNIC種別の右側にある「**編集**」ボタンをクリックします。

新しい「**NIC種別名**」を入力します。
入力が完了したら、「**変更**」ボタンをクリックし完了です。

12-2-3. NIC種別の削除

削除したいNIC種別の右側にある「**削除**」ボタンをクリックします。



確認ダイアログが表示されますので、「**はい**」をクリックし削除完了です。

※初期設定で「その他」と設定されている項目は削除することはできません。

13. ファームウェア管理

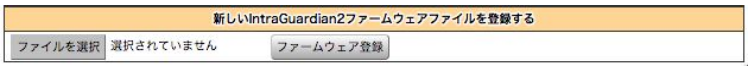
マネージャメニューの**ファームウェア管理**画面では、IntraGuardian本体 に現在インストールされているファームウェアを確認し、バージョンアップを行うことが可能です。

上部には、設置されている全IntraGuardianに現在インストールされているファームウェアのバージョン名が表示されます。
一方、下部には本ソフトウェアにアップロードされた IntraGuardian本体用ファームウェアファイルの一覧が表示されます。

13-1. ファームウェアファイルの登録

本ソフトウェアから IntraGuardian本体のファームウェアをバージョンアップするためには、まず、IntraGuardian本体用のファームウェアファイルを本ソフトウェアにアップロードして登録しておく必要があります。

サポートページ (https://intraguardian.jp)から IntraGuardian本体用ファームウェアファイルをダウンロードしておきます。(ファームウェアファイルのダウンロードには、ご登録いただいたIDが必要です。)
ファームウェア管理画面の下部にある「**ファイルを選択**」(ブラウザによっては「**参照...**」)と書かれた欄に、このダウンロードファイルを指定した上で、「**ファームウェア登録**」ボタンをクリックします。

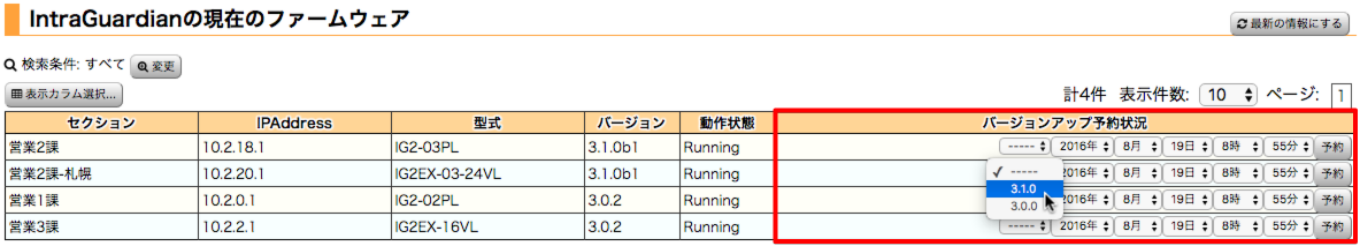


※ 本ソフトウェアはファイル名からバージョン番号や適用できるIntraGuardianのモデルを識別しますので、ダウンロードしたファイルのファイル名は変えないでください。

この時点では、ファームウェアファイルは本ソフトウェアのハードディスク上にコピーされただけで、まだ IntraGuardian本体には送付されていません。

13-2. ファームウェアの更新予約

各セクションごとにファームウェアの更新予約をすることができます。「**バージョンアップ予約状況**」にアップデートするファームウェアバージョンと更新を行う「**日時**」を選択し「**予約**」ボタンをクリックします。



指定した日時を過ぎると、本ソフトウェアは IntraGuardian本体と通信をする度に予約されたバージョンと一致しているかどうか確かめ、一致していなければファームウェアファイルを送信してアップデートを要求します。(一致していればバージョンアップ予約は取り消されます。)

※ 現在通信していないIntraGuardianに対してもバージョンアップ予約をすることができます。この場合、予約日時をすぎてから通信を開始次第、バージョンアップ作業が行われます。

また、検索条件に合致するすべてのIntraGuardianを一括更新指定することができます。

14. 登録申請機能

14-1. 登録申請機能とは

IntraGuardian2*(IG2-03PL, IG2EX-03-08VL, IG2EX-03-24VL) と本ソフトウェアを組み合わせると、登録申請機能を利用することが可能です。

登録申請機能とは、不正接続として検知された端末でウェブアクセスを行おうとしたときに、管理者宛に申請要求を出すことができる機能です。

登録申請機能が設定されているとき、排除されているPCでウェブブラウザを使って任意のページにアクセスしようとすると、（アクセス先のURLがどのようなものであっても）強制的に本ソフトウェアが生成した左図のような画面が表示されます。

端末利用者がこのフォームに必要事項を記入し「送信」をクリックすると、管理者に登録申請が出された旨の通知が送られます。

管理者は申請内容を確認した上で、申請を受領すると、当該端末が登録端末として取り扱われるようになります。（端末がネットワークに自由にアクセスできるようになります。）

※ 本機能は、不正接続端末のOSやブラウザの種類や設定状態によっては有効に機能しない場合があります。

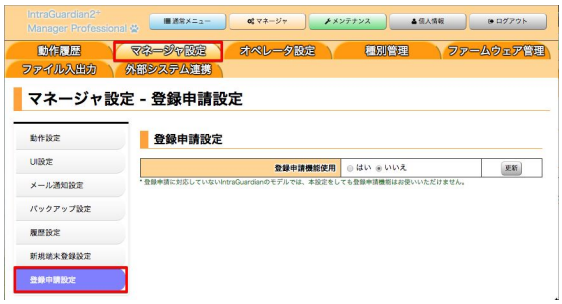
※ 本機能が有効なときに、登録済み端末から不正接続端末に対してHTTP接続をしようとすると申請画面が表示されます。

14-2. 登録申請機能の設定

登録申請機能を利用できるようにするためには、本マネージャの設定と、IntraGuardian本体の設定の両方を調整する必要があります。

14-2-1. マネージャ設定

マネージャメニューの**マネージャ設定**画面を開き、「**登録申請設定**」を選択します。

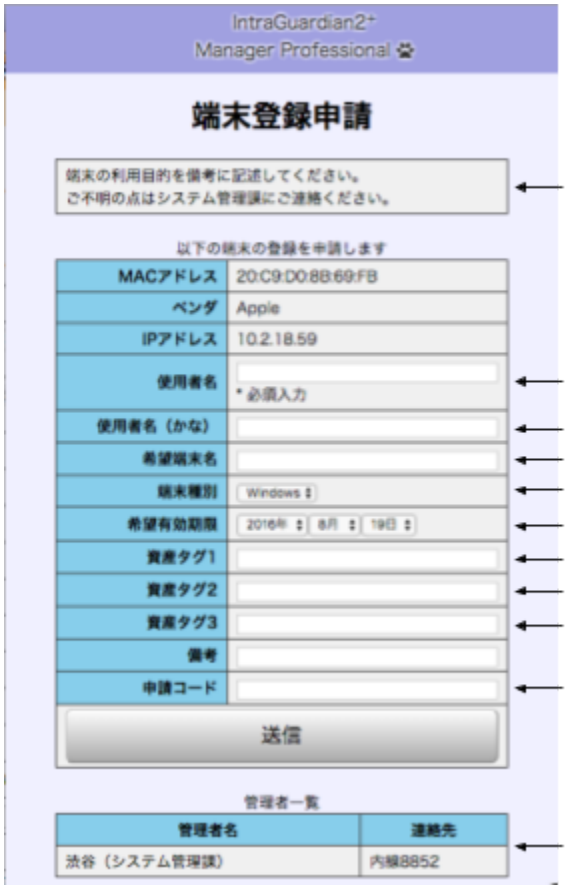


「**登録申請機能使用**」の「**はい**」を選択して「**更新**」をクリックすると、左図のように詳細な設定項目が入力できるようになりますので、各欄を入力して「**更新**」をクリックしてください。

＜登録申請設定項目＞

申請前メッセージ	不正接続端末のウェブブラウザに表示されるメッセージを指定します。
申請後メッセージ	申請送信後に表示されるメッセージを指定します。
端末名の入力 **所有者の入力** **所有者かなの入力** **デバイス種別の入力** **有効期限の入力** **資産タグ1の入力** **資産タグ2の入力** **資産タグ3の入力**	登録申請画面に各項目の入力欄を表示するかどうかを指定します。
管理者連絡先の表示	管理者の連絡先を不正接続端末に表示するかを指定します。
申請コード	申請するためにコードが必要かどうかを設定できます。 空欄の場合はコード入力無しで申請でき、入力した場合はコードが一致しない場合申請を受け付けません。
登録申請画面で用いる時間帯	有効期限を入力させるときに使う時間帯を指定します。
最大同時申請数	登録申請画面に対して異常アクセスがされたときに備え、登録申請がこの個数以上溜まったら登録申請機能を一時的に無効にします。
ロゴ画像PNGファイル	端末登録申請画面にロゴ画像を表示することができます。PNGファイルを指定してます。

＜登録申請画面（不正端末に表示される）＞



申請前メッセージを入力するとここに表示される

所有者名の入力欄

所有者名（かな）の入力欄

端末名の入力欄

デバイス種別の入力欄

有効期限の入力欄

資産タグ1の入力欄

資産タグ2の入力欄

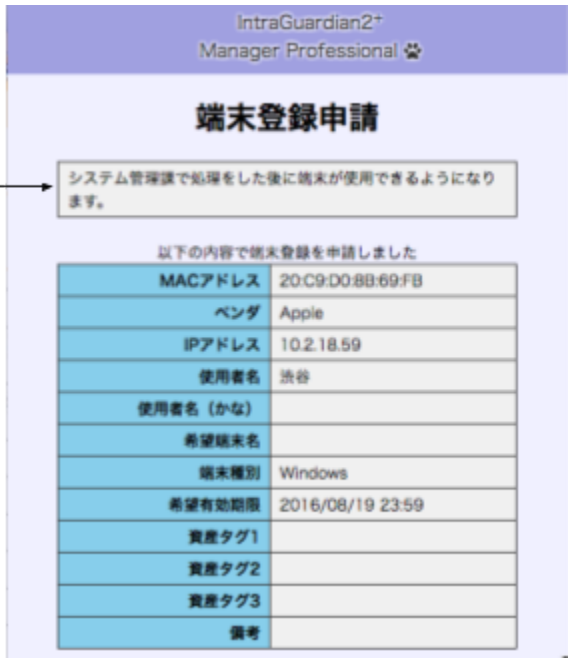
資産タグ3の入力欄

申請コードの入力欄（申請コードが空白の場合表示されない）

管理者連絡先の表示

＜登録申請後画面（不正端末に表示される）＞

申請後メッセージを入力するとここに表示される



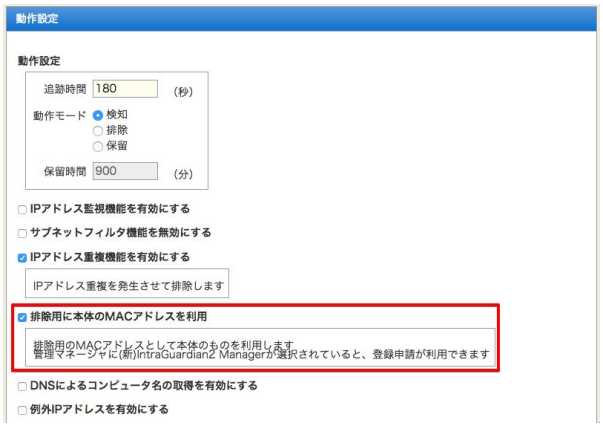
14-2-2. 監視設定（IntraGuardian設定）

IntraGuardian本体側の設定項目にも登録申請を有効にする項目がありますので、そちらも設定します。

登録申請機能を利用したいセクションを選択した状態で**通常メニューの監視設定**画面を開き、「**基本設定**」を選択します。
「検知・排除方式」の欄に「端末登録申請」の項目がありますので、「有効」を選択して更新します。

※ 本設定をしても IG2-03PL, IG2EX-03-08VL, IG2EX-03-24VL 以外のモデルの IntraGuardianでは登録申請機能は使用できません。

本設定を有効にすると、IntraGuardian本体のUI画面上では、「排除用に本体のMACアドレスを利用」が選択された状態になります。

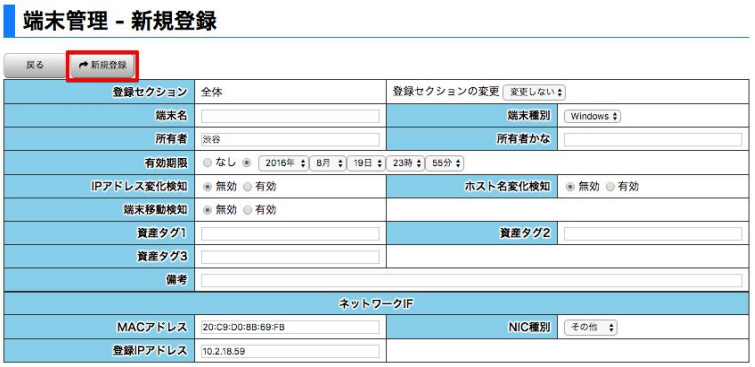


もし、本設定を有効にして、マネージャ設定の登録申請機能を無効にしている場合、不正端末のWEBブラウザには次の表示がでます。

14-3. 登録申請一覧

マネージャ設定で登録申請機能が有効になっていると、**通常メニュー**のサブメニューに「**登録申請一覧**」が表示されます。
この画面を表示すると、着目しているセクション（およびその子孫セクション）で申請されている端末を一覧できます。

表の1行をクリックするか、右端の「登録」ボタンをクリックすると、端末管理画面の新規登録画面が表示されます。



登録申請者が指定した情報がある場合は、その内容があらかじめ入力された状態になっていますので、必要に応じて内容を書き換えるなどして「新規登録」ボタンをクリックすると、この端末が登録され、1分程度のうちに登録情報がIntraGuardianに送信されます。
IntraGuardianはこの端末に対する排除処理をやめますので、この端末は普通にネットワークアクセスを行うことができるようになります。
（**ただし、当該端末やルータなどのネットワーク機器が記憶した偽のARP情報を完全に忘れるまでの間（一般的には数分程度）は、ネットワークへのアクセスが不安定になることがあります。**）

申請が不正なものであり許可できない場合は、登録申請一覧画面で「**拒否**」ボタンをクリックしてください。

拒否ボタンをクリックすると確認の画面が表示されるので、本当に拒否する場合は「**はい**」ボタン、間違いだった場合は「**いいえ**」ボタンをクリックしてください。

登録か拒否をするまで、申請情報はずっと残り続けます。

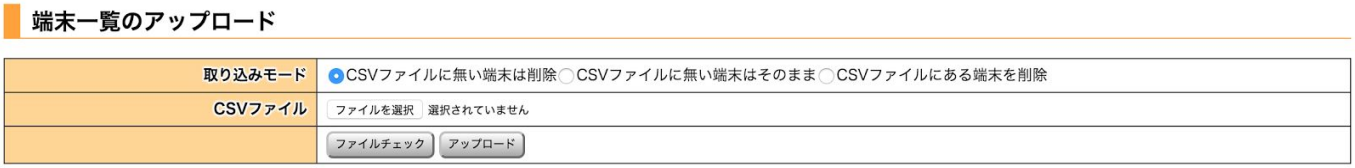
15. ファイル入出力

マネージャメニューのファイル入出力画面を使うと、全登録端末の一覧と全セクションの一覧をテキストファイル形式で入出力することができます。
登録端末一覧は CSVフォーマットで、セクション情報の一覧は XMLフォーマットでファイル化されます。

15-1. 端末一覧のダウンロード

ダウンロードボタンをクリックすると、現在の登録端末の一覧をCSVとして出力することが可能です。CSVのフォーマットは、後述する「端末CSVファイルフォーマット」で指定することができます。

15-2. 端末一覧のアップロード



原則として、「端末一覧のダウンロード」で生成されたCSVファイルを取り込む機能です。

取り込むCSVファイルは、次の基本フォーマットに従っていなければいけません。

- 文字コードは「CSVフォーマットオプション」の「文字エンコード」で指定したコードを用います。
  ASCIIやShift-JISなどを含む多くの文字コードが指定できますが、システム内部ではUNICODEを用いているため、UTF-8などのUNICODEを全てサポートするコードをお使いになることを強くお勧めします。
  万が一指定した文字コードで正しく表現できない文字（機種依存文字など）がCSVファイル中にある場合、文字化けまたは文字コード変換エラーが発生し、正しく取り込むことができません。
  なお、UTF-8を用いる場合のBOMコードは、あってもなくても構いません。
- 改行コードはCR、LF、CR+LFのいずれでもかまいません。
- カラム区切り文字は','（カンマ）固定です。カンマの前後の空白文字は全て読み飛ばされます。
- 行の最初の文字が'#'（ナンバ記号）である場合、その行はコメント行として読み飛ばされます。
  ただし、1行目が'#'で始まっている場合、その行はカラムの並び順を規定する行として特別処理されます。（カラム指定については次項で詳しく説明いたします。）
- 空行は全て読み飛ばされます。
- 各カラムの値が '"'（ダブルクォート）または"'"（シングルクォート）で囲まれている場合、このクォート文字は無視されます。
- '\'（バックスラッシュ）は、すぐ次の文字を特殊文字として取り扱わないエスケープ文字として取り扱われます。すなわち、カラムの先頭の文字が"である場合には\"と記述します。また、カラムの値にバックスラッシュを含めたい場合には\\と記述します。
- カラムの値に ','（カンマ）が含まれる場合には、カラム値をクォート文字で囲うか、\,とカンマをエスケープしなければいけません。

アップロードする際は「**ファイルを選択**」（ブラウザによっては「**参照...**」）でCSVファイルを指定してから、「**アップロード**」ボタンをクリックします。
「**ファイルチェック**」をクリックした場合、フォーマットのチェックだけ行い、実際の登録一覧には適用されません。

登録端末一覧CSVファイルを取り込ませる際には、次の取り込みモードを選択することができます。

1. CSVファイルに無い端末は削除
2. CSVファイルに無い端末はそのまま
3. CSVファイルにある端末を削除

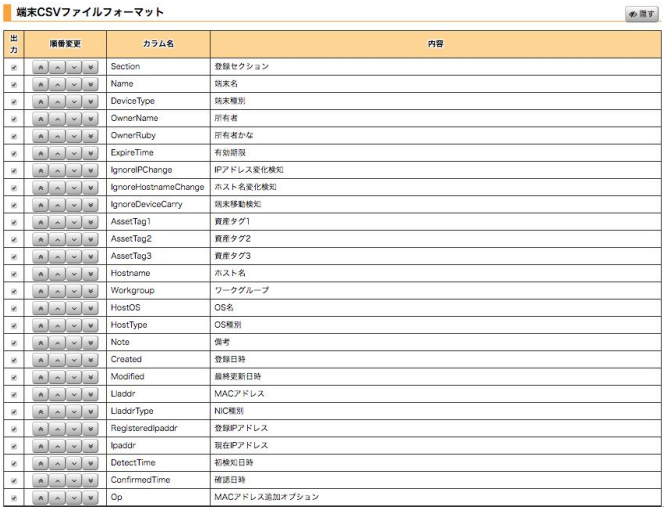
1.のモードを用いると、登録端末一覧をそっくり入れ直すことができます。
2.のモードでは、追加する端末だけを記述したCSVを取り込ませることができます。
3.のモードを用いる場合、CSVファイル中の端末名以外の項目は全て無視され、指定された端末の登録が削除されます。

15-3. CSVファイルフォーマット

上記のCSVファイル入出力で用いられるファイルのフォーマットの詳細は、「端末CSVファイルフォーマット」欄で変更することができます。（項目数が多いため、デフォルトの状態では本欄は非表示になっています。「表示する」ボタンをクリックすると内容が表示されます。）

端末CSVファイルフォーマットの上の部分は、出力する項目の選択とその並び順の指定です。
「出力」欄にチェックマークをつけると出力され、チェックマークを消すと出力されません。

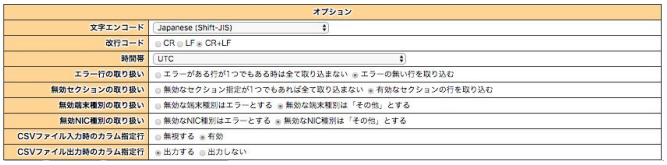
をクリックすると順番を変更できます。左から順番に「最も先頭」「一つ前」「一つ後」「最も最後」に移動します。



「MACアドレス追加オプション」項目は、1つの端末に複数のネットワークIFが存在する（複数のMACアドレスを持つ）場合に必要となります。
通常、同じ端末名を持つ行が複数ある場合、後の方の行のデータで内容は上書きされます。
しかし、「MACアドレス追加オプション」欄が存在し、そこに '+'（プラス記号）が記述されている場合、「MACアドレス」「MACアドレス種別」「登録IPアドレス」については上書きではなく、追加の意味で処理されます。
MACアドレス追加オプション欄が存在しても、そこが空欄の場合には、「MACアドレス」「MACアドレス種別」「登録IPアドレス」についても上書きとして処理されます。また、これら以外の項目については、MACアドレス追加オプションの記述にかかわらず常に上書きとして処理されます。
なお、将来の拡張に対する互換性を確保するため、MACアドレス追加オプション欄には'+'以外を記述しないようにしてください。

CSVファイルの1行目が'#'で始まっていない場合、またはCSVフォーマットオプションの「CSVファイル入力時のカラム指定行」に「無視する」が指定されている場合、各行はCSVフォーマットオプションで指定されたカラム順にデータが並んでいるものとして処理されます。
万が一、各行のデータの個数が指定されたカラム数よりも少ない場合、足りないカラムは空欄が指定されたもの（デフォルト値が指定されたもの）として処理されます。

端末CSVファイルフォーマットの下部は、フォーマットに関するオプション設定です。
次のオプションでエラー処理などの挙動を指定することができます。



オプション	内容
文字エンコード	入出力に用いる文字コード。
改行コード	出力に用いる文字コード。入力時はCR / LF / CR+LF のいずれでも構いません。
時間帯	登録日時などの解釈に用いる時間帯。
エラー行の取り扱い	入力の際にエラーが発生したときの動作。 エラーがある行が1つでもある時は全て取り込まない ／ エラーの無い行を取り込む
無効セクションの取り扱い	入力の際に登録されていないセクション名が存在したときの動作。 無効なセクション指定が1つでもあれば全て取り込まない ／ 有効なセクションの行を取り込む
無効端末種別の取り扱い	入力の際に登録されていない端末種別が存在したときの動作。 無効な端末種別はエラーとする ／ 無効な端末種別は「その他」とする
無効NIC種別の取り扱い	入力の際に登録されていないNIC種別が存在したときの動作。 無効なNIC種別はエラーとする ／ 無効なNIC種別は「その他」とする

CSVファイル入力時のカラム指定行	入力の際に1行目のカラム指定を無視するかどうか。
CSVファイル出力時のカラム指定行	出力の際に1行目のカラム指定を出力するかどうか。

なお、「無効セクションの取り扱い」の設定状態に関わらず、セクション名が指定されない場合（セクション名カラムが無い場合、またはセクション名が空欄である場合）には、「全体」セクションが指定されたものとして取り扱われます。

15-4. セクション情報のダウンロード

ダウンロードボタンをクリックすると、現在の全セクション情報をXMLとして出力することが可能です。
このセクション情報出力には、セクション名、セクションの階層構造、ネットワーク設定、対応IGとその設定、例外アドレス情報、管理／閲覧オペレータ情報が含まれます。

XML version 1.0で文字コードはUTF-8です。
ルート要素は 'ig2mla' で、このルート要素の中に 'section'要素と'operator'要素が複数含まれます。
'section'要素内には、親セクションを示す'parent'要素、管理者を示す'operator'要素、対応IGを示す'ig'要素、ネットワーク設定を示す'network'要素、例外ベンダを示す'exceptional-lladdr'要素、例外IPアドレスを示す'exceptional-ip'要素が含まれます。
各要素の内容はすべてタグの属性として表記され、TEXTノードはすべて無視されます。（出力の際には、読みやすくするための改行と空白だけがTEXTノードに含まれます。）
'parent'要素を持たないセクションはルートセクション（全体セクション）として扱われます。このルートセクションは1つしか存在してはいけません。

XMLで用いられる各タグの定義は次の通りです。

タグ名: **ig2mla**
ルート要素。

上位タグ	なし
下位タグ	section, operator

属性名		説明
version		IG2MLAバージョン番号
created		XML作成日時。YYYY/MM/DD HH:MM:SS 形式。UTC

タグ名: **section**
セクション定義。

上位タグ	ig2mla
下位タグ	parent, operator, network, ig, exceptional-ip, exceptional-lladdr

属性名		説明
name	必須	セクション名
note		備考

タグ名: **parent**
親セクション指定。
当該セクション名はすでに定義されたものでなければならない。
ルートセクション以外では必ず1つ以上存在しなければならない。

上位タグ	section
下位タグ	なし

属性名		説明
name	必須	セクション名

タグ名: **operator**
オペレータ定義。
section要素内に現れた場合は、そのセクションの管理／閲覧者であることを示す。

上位タグ	ig2mla, section
下位タグ	notify

属性名		説明
login	必須	ログインID
role		権限 (Observer/Admin/SysAdmin/Super)デフォルトは Observer
name		名前
password		パスワードをハッシュコード化したもの
mail		メールアドレス
contact		連絡先
timezone		時間帯
lang		言語 (ja/en)
note		備考

タグ名: **notify**
オペレータの通知定義。
本要素が存在する場合、当該オペレータへの通知が行なわれる。

上位タグ	operator
下位タグ	なし

属性名		説明
method	必須	通知種別（現在は MAIL のみ）
event	必須	イベントコード

タグ名: **network**
ネットワーク定義

上位タグ	section
下位タグ	なし

属性名		説明
address	必須	(IGの)IPアドレス
netmask	必須	ネットマスク。xxx.xxx.xxx.xxx形式
gateway		ゲートウェイアドレス
lgateway		ローカルゲートウェイアドレス
dns		DNSサーバアドレス（複数ある場合は','で区切って並べる）

gateway属性とlgateway属性を同時に指定してはいけない。

タグ名: **ig**
IntraGuardian定義

上位タグ	section
下位タグ	category

属性名		説明

id	必須	IGID。'#'+16進数8桁

タグ名: **category**
IntraGuardian設定カテゴリ。
当該カテゴリ内の設定値がすべてデフォルト値の場合にはcategory要素は出力されない。

上位タグ	ig
下位タグ	config

属性名		説明
name	必須	カテゴリ名。Network/Mode/Advanced/Notify

タグ名: **config**
IntraGuardian設定。
当該項目の設定値がデフォルト値の場合にはconfig要素は出力されない。

上位タグ	category
下位タグ	なし

属性名		説明
name	必須	設定項目名
value	必須	設定値

タグ名: **exceptional-ip**
例外IPアドレス。

上位タグ	section
下位タグ	なし

属性名		説明
address		例外IPアドレス。単一指定の場合。
start		例外IPアドレス範囲開始アドレス
end		例外IPアドレス範囲終了アドレス

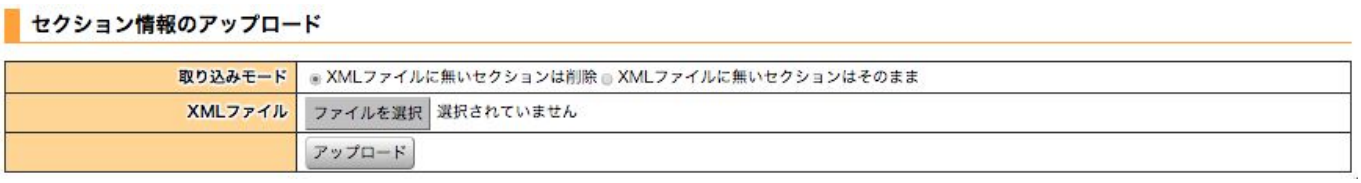
address属性またはstart属性のいずれかがなければならない。
start属性がある場合にはend属性は必須。

タグ名: **exceptional-lladdr**
例外ベンダアドレス。

上位タグ	section
下位タグ	なし

属性名		説明
address	必須	例外ベンダアドレス。単一指定の場合。XX:XX:XX形式

15-5. セクション情報のアップロード



原則として、「セクション情報のダウンロード」で生成されたXMLファイルを取り込む機能です。
アップロードする際は「**ファイルを選択**」(ブラウザによっては「**参照...**」)でXMLファイルを指定してから、「**アップロード**」ボタンをクリックします。

セクション情報XMLファイルを取り込ませる際には、次の取り込みモードを選択することができます。

1. XMLファイルに無いセクションは削除
2. XMLファイルに無い端末はそのまま

1.のモードを用いると、全セクションをそっくり入れ直すことができます。
2.のモードでは、追加するセクションだけを記述したXMLを取り込ませることができます。

16. 外部システム連携

マネージャメニューの**外部システム連携**画面を使うと、【14. ファイル入出力】と同様のことを、自動で行うことができます。
資産管理ソフトウェアなどとの連携にご利用ください。
※本画面は、クラウド版マネージャをご利用の場合は操作できません。

16-1. 端末一覧書き出し

16-1-1. 指定ディレクトリへの保存

端末一覧CSVファイルを、定時に特定のディレクトリ内に出力させることができます。

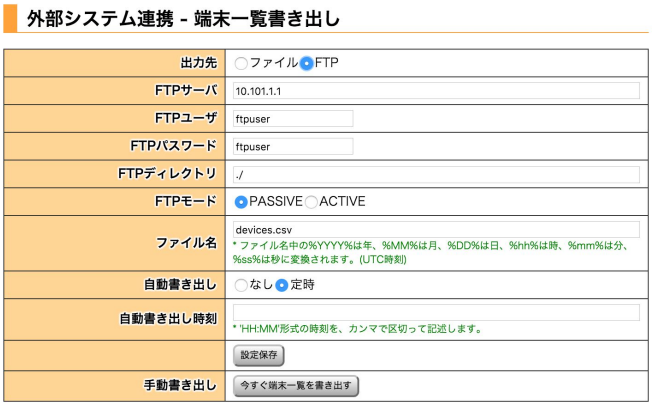
ディレクトリ	出力先ディレクトリを指定します。 サーバー上に保存したい場合は、FTPをご利用ください。
ファイル名	ファイル名を指定できます。 ファイル名の中には変数が指定できます。 %YYYY%は年 %MM%は月 %DD%は日 %hh%は時 %mm%は分 %ss%は秒に変換されますが、すべてUTC時刻になることに注意してください。
自動書き出し	定時を指定すると、指定された時刻に毎回CSVを出力することが可能です。
自動書き出し時刻	HH:MM形式の時刻をカンマ区切りで指定できます。

出力先を「**ファイル**」にして、ディレクトリとファイル名を指定してから「**設定保存**」ボタンをクリックしてください。
「**今すぐ端末一覧を書き出す**」ボタンをクリックすると、自動的にではなく今の情報がすぐに書き出されます。

運用のテストにご利用ください。

16-1-2. FTPへの保存

端末一覧CSVファイルを、定時にFTPサーバにアップロードさせることができます。



FTPサーバ	FTPサーバをIPアドレスもしくはホスト名で指定してください。
FTPユーザ	FTPサーバのユーザ名を指定してください。
FTPパスワード	FTPサーバのパスワードを指定してください。
FTPディレクトリ	ファイルを書き出すディレクトリを指定してください。
FTPモード	パッシブ/アクティブが指定できます。
自動書き出し	定時を指定すると、指定された時刻に毎回CSVを出力することが可能です。
自動書き出し時刻	HH:MM形式の時刻をカンマ区切りで指定できます。

出力先を「**FTP**」にして、FTPの各パラメータを指定してから「**設定保存**」ボタンをクリックしてください。
「**今すぐ端末一覧を書き出す**」ボタンをクリックすると、自動的にではなく今の情報がすぐに書き出されます。
運用のテストにご利用ください。

16-2. 端末一覧取り込み

16-2-1. 指定ディレクトリからの取り込み

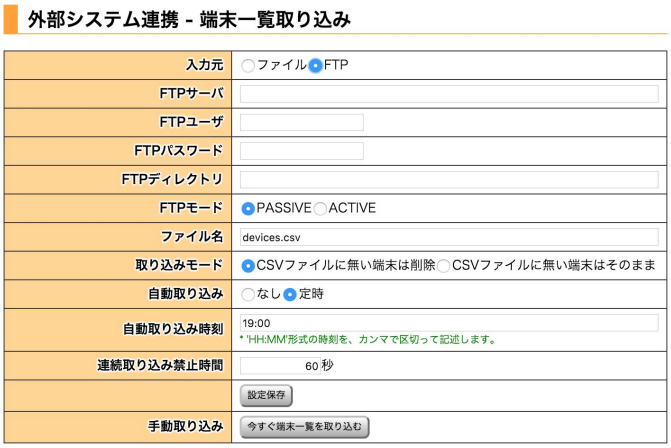
書き出し同様に、端末一覧の取り込みについても自動的に行えます。

ディレクトリ	入力元ディレクトリを指定します。 サーバー上のファイルを利用したい場合は、FTPをご利用ください。
ファイル名	ファイル名を指定します。
取り込みモード	端末登録をCSVの内容で置き換えるか、CSVの内容を追加登録として取り扱うかを指定します。
自動取り込み	定時を指定すると、指定された時刻に毎回CSVを取り込むことが可能です。
自動取り込み時刻	HH:MM形式の時刻をカンマ区切りで指定できます。
連続取り込み禁止時間	自動取り込み処理と手動取り込み処理が連続して発生することにより端末情報が破壊される可能性を避けるためのガードタイムです。

入力元を「**ファイル**」にして、ディレクトリとファイル名を指定してから「**設定保存**」ボタンをクリックしてください。
「**今すぐ端末一覧を取り込む**」ボタンをクリックすると、自動的にではなく今の情報がすぐに書き出されます。
運用のテストにご利用ください。

16-2-2. FTPからの取り込み

端末一覧の取り込みをFTPから行う場合の設定です。



FTPサーバ	FTPサーバをIPアドレスもしくはホスト名で指定してください。
FTPユーザ	FTPサーバのユーザ名を指定してください。
FTPパスワード	FTPサーバのパスワードを指定してください。
FTPディレクトリ	FTPサーバ上のディレクトリを指定してください。
FTPモード	パッシブ/アクティブが指定できます。

ファイル名	ファイル名を指定してください。
取り込みモード	端末登録をCSVの内容で置き換えるか、CSVの内容を追加登録として取り扱うかを指定します。
自動取り込み	定時を指定すると、指定された時刻に毎回CSVを取り込むことが可能です。
自動取り込み時刻	HH:MM形式の時刻をカンマ区切りで指定できます。
連続取り込み禁止時間	自動取り込み処理と手動取り込み処理が連続して発生することにより端末情報が破壊される可能性を避けるためのガードタイムです。

出力先を「**FTP**」にして、FTPの各パラメータを指定してから「**設定保存**」ボタンをクリックしてください。
「**今すぐ端末一覧を書き出す**」ボタンをクリックすると、自動的にではなく今の情報がすぐに書き出されます。
運用のテストにご利用ください。

16-3. 端末CSVフォーマット

端末一覧の入出力に用いるCSVのフォーマットオプションを指定できます。
設定内容は【14-3. CSVフォーマット】と同じですので、そちらをご覧ください。

16-4. 端末一覧書き出し

16-4-1. 指定ディレクトリへの保存

セクション情報XMLファイルを、定時に特定のディレクトリ内に出力させることができます。

ディレクトリ	出力先ディレクトリを指定します。 サーバー上に保存したい場合は、FTPをご利用ください。
ファイル名	ファイル名を指定できます。 ファイル名の中には変数が指定できます。 %YYYY%は年 %MM%は月 %DD%は日 %hh%は時 %mm%は分 %ss%は秒に変換されますが、すべてUTC時刻になることに注意してください。
自動書き出し	定時を指定すると、指定された時刻に毎回ファイルを出力することが可能です。
自動書き出し時刻	HH:MM形式の時刻をカンマ区切りで指定できます。

出力先を「**ファイル**」にして、ディレクトリとファイル名を指定してから「**設定保存**」ボタンをクリックしてください。
「**今すぐセクション情報を書き出す**」ボタンをクリックすると、自動的にではなく今の情報がすぐに書き出されます。
運用のテストにご利用ください。

16-4-2. FTPへの保存

セクション情報XMLファイルを、定時にFTPサーバにアップロードさせることができます。

FTPサーバ	FTPサーバをIPアドレスもしくはホスト名で指定してください。
FTPユーザ	FTPサーバのユーザ名を指定してください。
FTPパスワード	FTPサーバのパスワードを指定してください。
FTPディレクトリ	ファイルを書き出すディレクトリを指定してください。
FTPモード	パッシブ/アクティブが指定できます。
自動書き出し	定時を指定すると、指定された時刻に毎回ファイルを出力することが可能です。

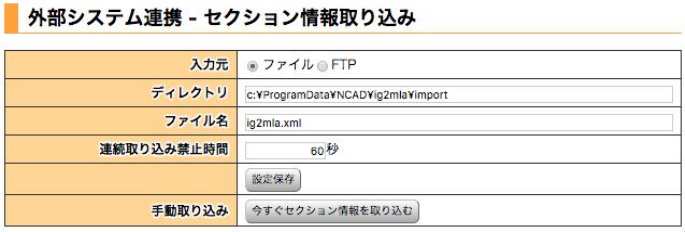
自動書き出し時刻	HH:MM形式の時刻をカンマ区切りで指定できます。

出力先を「**FTP**」にして、FTPの各パラメータを指定してから「**設定保存**」ボタンをクリックしてください。
「**今すぐセクション情報を書き出す**」ボタンをクリックすると、自動的にではなく今の情報がすぐに書き出されます。
運用のテストにご利用ください。

16-5. セクション情報取り込み

16-5-1. 指定ディレクトリからの取り込み

※ 現在、セクション情報の取り込みについては定時実行することはできません。

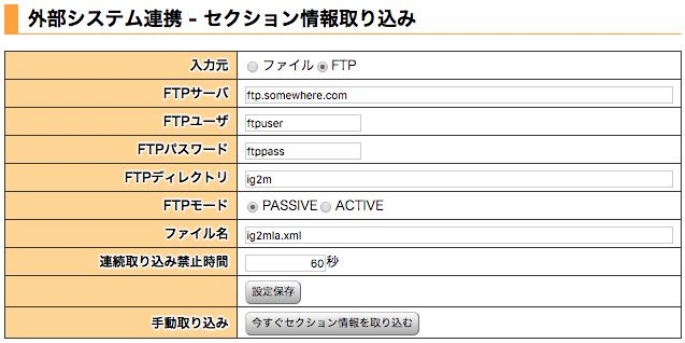


ディレクトリ	入力元ディレクトリを指定します。 サーバー上のファイルを指定したい場合は、FTPをご利用ください。
ファイル名	ファイル名を指定します。
連続取り込み禁止時間	自動取り込み処理と手動取り込み処理が連続して発生することにより端末情報が破壊される可能性を避けるためのガードタイムです。

入力元を「**ファイル**」にして、ディレクトリとファイル名を指定してから「**設定保存**」ボタンをクリックしてください。
「**今すぐセクション情報を取り込む**」ボタンをクリックすると、今の情報がすぐに書き出されます。

16-5-2. FTPからの取り込み

端末一覧の取り込みをFTPから行う場合の設定です。



FTPサーバ	FTPサーバをIPアドレスもしくはホスト名で指定してください。
FTPユーザ	FTPサーバのユーザ名を指定してください。
FTPパスワード	FTPサーバのパスワードを指定してください。
FTPディレクトリ	FTPサーバ上のディレクトリを指定してください。
FTPモード	パッシブ/アクティブが指定できます。
ファイル名	ファイル名を指定してください。
連続取り込み禁止時間	自動取り込み処理と手動取り込み処理が連続して発生することにより端末情報が破壊される可能性を避けるためのガードタイムです。

出力先を「**FTP**」にして、FTPの各パラメータを指定してから「**設定保存**」ボタンをクリックしてください。
「**今すぐセクション情報を書き出す**」ボタンをクリックすると、今の情報がすぐに書き出されます。

17. バックアップ・復元

メンテナンスメニューの**バックアップ・復元**画面を使うと、本ソフトウェアが使っているデータベース内容のバックアップ・復元を行うことができます。バックアップには、「**ブラウザにダウンロード**」、「**本ソフトウェアを保存している環境内に保存**」、「**FTPによる保存**」を選択することができます。

※クラウド版マネージャでは、バックアップディレクトリはご利用できません。

17-1. バックアップのダウンロード

現在の設定を一つのファイルにバックアップし、手元（操作している環境）にダウンロードすることができます。

1. バックアップ先を「**ダウンロード**」を選択
2. バックアップ内容を選択

全部	全て（※1）のデータをバックアップ対象とする
古い履歴を除く	最近の履歴とする日数（※2）を超える履歴を除く全てのデータをバックアップ対象とする
履歴を全て除く	履歴データ（動作履歴、端末履歴）を除くデータをバックアップ対象とする

※1 履歴データを含むと大きなデータになるのでご注意ください
※2 最近の履歴とする日数は「マネージャ設定」の「履歴設定」の値です

3. バックアップファイルを暗号化するためのキーを入力
   ※暗号化しない場合は入力なし
4. 「**ダウンロード**」ボタンをクリック
5. バックアップファイルがダウンロードされます

17-2. バックアップのファイル保存

本ソフトウェアをセットアップしたPC上にバックアップファイルを作成する機能です。作成されるファイルは「**バックアップのダウンロード**」と同様のファイルです。

1. バックアップ先を「**ファイル保存**」を選択
2. バックアップ内容を選択（**※前述確認**）
3. バックアップファイルを暗号化するためのキーを入力
4. ディレクトリへ保存先ディレクトリを**フルパス**（**絶対パス**）で指定
5. 「**ファイル作成**」ボタンをクリック
6. バックアップファイルが保存されます

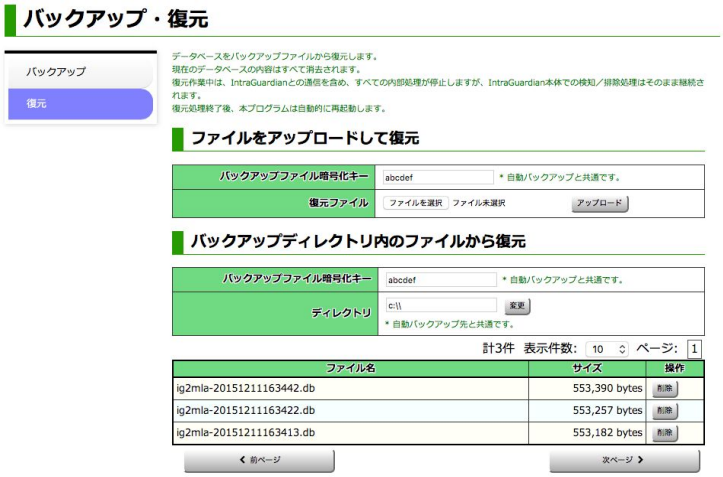
17-3. バックアップのFTP保存

バックアップファイルをFTPサーバに作成する機能です。作成されるファイルは「**バックアップのダウンロード**」と同様のファイルです。

1. バックアップ先を「**FTP保存**」を選択
2. バックアップ内容を選択（**※前述確認**）
3. バックアップファイルを暗号化するためのキーを入力
4. **FTPサーバ**のアドレスを入力
   ※ホスト名指定をする場合はセットアップPCからの名前解決をご確認の上ご利用ください
5. **FTPユーザ**、**FTPパスワード**を入力
6. **FTPディレクトリ**を入力
7. **FTPモード**を「**パッシブ**（**アクティブ**）」を選択
8. 「**実行**」ボタンをクリック
9. バックアップファイルがFTPサーバにアップロードされます

17-4. 復元

自動バックアップまたは、手動バックアップにて作成されたバックアップファイルから設定を復元します。復元をおこなうと、**現在のデータベースの内容はすべて消去されます。また、復元作業中はIntraGuardianとの通信を含め、すべての内部処理が停止しますが、IntraGuardian本体での検知／排除処理はそのまま継続されます。復元処理完了後、本ソフトウェアは自動的に再起動を行い復元したデータで動作を開始します。**



17-4-1. ファイルをアップロードして復元

バックアップファイルのダウンロードまたは、手動、自動バックアップのFTP保存等されたバックアップファイルから復元を行う際に利用します。

1. **バックアップファイルの暗号化キー（暗号化されていない場合は入力なし）**を入力
2. 復元ファイルを指定
3. 「**アップロード**」ボタンをクリック
4. 復元処理完了です

※復元処理には復元データによっては時間がかかる場合があります。復元の際にはご注意ください。

17-4-2. バックアップディレクトリ内のファイルから復元

本ソフトウェアをセットアップしたPC上にバックアップされた**バックアップファイルから復元**をおこないます。

1. **バックアップファイルの暗号化キー**(**暗号化されていない場合は入力なし**)を入力
2. 一覧に表示されているバックアップファイルをダブルクリックすると復元が開始されます

※ディレクトリを変更する場合は、ディレクトリのパスを入力し「変更」ボタンをクリックし変更します。

17-5. 自動バックアップ設定

マネージャ設定画面の「**バックアップ設定**」を使うと、上述のバックアップを自動で行わせることができます。

※自動バックアップの設定は「メンテナンス」の「バックアップ復元」ではなく「マネージャ」の「マネージャ設定」にあります。

※本画面は、クラウド版マネージャをご利用の場合は操作できません。

17-5-1. ファイル保存方式の自動バックアップ

自動バックアップの設定内容は、「**メンテナンス**」の「**バックアップ復元**」と同じになります。

※メンテナンスと別の設定を入れることはできません。

1. 自動バックアップを「はい」を選択し右側の「**更新**」ボタンをクリック
2. 自動バックアップ時刻を選択し右側の「**更新**」ボタンをクリック
3. バックアップ先を「**ファイル保存**」を選択し右側の「**更新**」ボタンをクリック
4. バックアップ内容を選択(**※前述確認**) し右側の「**更新**」ボタンをクリック
5. バックアップファイルを暗号化するためのキーを入力し右側の「**更新**」ボタンをクリック
6. ディレクトリへ保存先ディレクトリを**フルパス**(**絶対パス**)で指定し右側の「**更新**」ボタンをクリック

上記でファイル保存の自動バックアップ設定完了です。

17-5-2. FTP保存方式の自動バックアップ

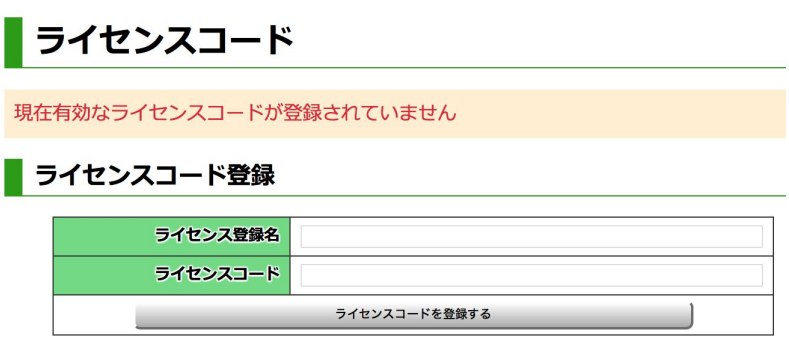
自動バックアップの設定内容は、「**メンテナンス**」の「**バックアップ復元**」と同じになります。
※メンテナンスと別の設定を入れることはできません。

1. 自動バックアップを「はい」を選択し右側の「**更新**」ボタンをクリック
2. 自動バックアップ時刻を選択し右側の「**更新**」ボタンをクリック
3. バックアップ先を「**FTP保存**」を選択し右側の「**更新**」ボタンをクリック
4. **FTPサーバ**のアドレスを入力し右側の「**更新**」ボタンをクリック　**※ホスト名指定をする場合はセットアップPCからの名前解決をご確認の上ご利用ください**
5. **FTPユーザ**、**FTPパスワード**を入力し右側の「**更新**」ボタンをクリック
6. **FTPディレクトリ**を入力し右側の「**更新**」ボタンをクリック
7. **FTPモード**を「**パッシブ**（**アクティブ**）」を選択し右側の「**更新**」ボタンをクリック

18. ライセンス登録

メンテナンスメニューのライセンスコード画面を使うと、本ソフトウェアのライセンスコードを登録することができます。
※本画面は、クラウド版マネージャをご利用の場合は操作できません。

使用開始直後はライセンスコードが未入力のため、「現在有効なライセンスコードが登録されていません」と表示されます。



正しい「ライセンス登録名」、「ライセンスコード」を入力し、「ライセンスコードを登録する」をクリックすると認証されます。

※ライセンス登録名は空白や全角／半角の違いを含め、申請されている名称と全く同じで登録しないと認証できませんのでご注意ください。

19. ソフトウェア更新

メンテナンスメニューの**アプリ更新**画面を使うと、本ソフトウェアをバージョンアップすることができます。
※本画面は、クラウド版マネージャをご利用の場合は操作できません。

19-1. アップグレードファイルの入手

本ソフトウェアのバージョンアップの際には、新規インストール用とは異なる「アップグレード用ファイル」が必要です。(アップグレード用ファイルのファイル名は拡張子 ".bin"で終わります。)
アップグレード用ファイルは、サポートサイト (https://intraguardian.jp) のダウンロードページから入手できます。(ただし、ライセンス登録時に発行されるIDとパスワードが必要です。)

無償版をお使いなどの理由でアップグレード用ファイルを入手できない場合は、古いバージョンを一度アンインストールしてから新しいバージョンをインストールしなおしてください。

19-2. バージョンアップ

全権管理者としてログインし、**メンテナンス**メニュー内の「**アプリ更新**」画面を表示します。
入手したアップグレード用ファイルを選択し、「**アップグレード**」ボタンをクリックしてください。

本プログラムファイルが更新され、自動的に再起動しますので、再度ログインしなおして動作をご確認下さい。

19-3. Windowsの再起動

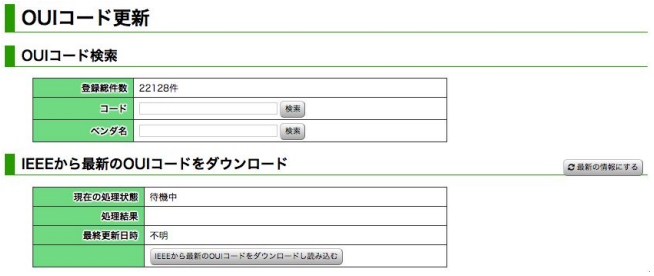
バージョンアップが完了したら、Windows内のDLLファイル管理情報などの整合を保つため、必ず一度Windowsを再起動してください。

20. OUIコード更新

OUIコードとは、MACアドレスの先頭3オクテットの数値で、NICのメーカ毎に割り当てられています。どのメーカがどのOUIコードを用いているかは IEEEが管理をしており、そのデータベースはインターネットに公開されています。

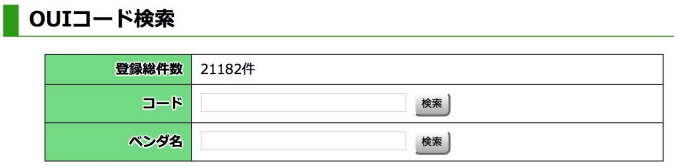
メンテナンスメニューのOUIコード更新画面を使うと、最新のデータベースをIEEEからダウンロードし、本ソフトウェアのデータベースに登録することができます。

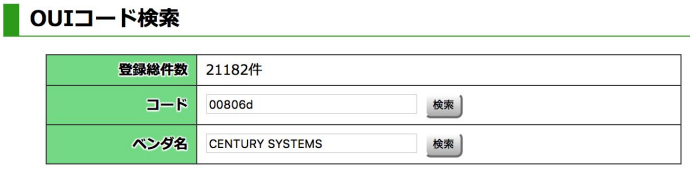
また、OUIコード検索では、現在適用されているデータからコードまたはベンダ名を検索しコードまたはベンダ名を表示します。



20-1. OUIコード検索

OUIコード検索は、コード（またはベンダ名）を入力し検索すると、ベンダ名（またはコード）を得ることができます。

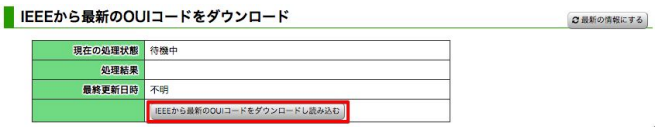


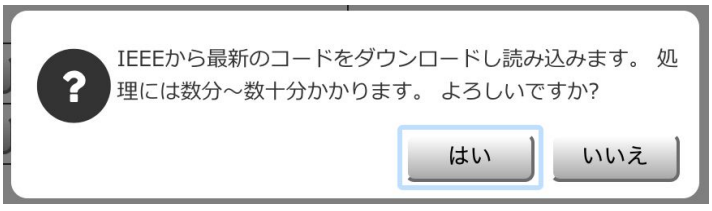


左図は、コードを入力し検索したところです。コードには、「:」（コロン）で区切らなくても検索可能です。

20-2. IEEEから最新のOUIコードをダウンロード

最新のOUIコードをダウンロードするには、右図の「**IEEEから最新のOUIコードをダウンロードし読み込む**」ボタンをクリックします。



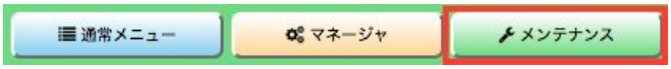


左図の確認ダイアログが表示されるので「**はい**」をクリックします。

21. アプリ情報

アプリケーションの動作状況を確認することができます。メンテナンス時に参考にする数値が表示されます。
※本画面は、クラウド版マネージャをご利用の場合は操作できません。

トップメニューの「**メンテナンス**」をクリックします。



メンテナンスの「**アプリ情報**」をクリックします。

21-1. バージョン情報

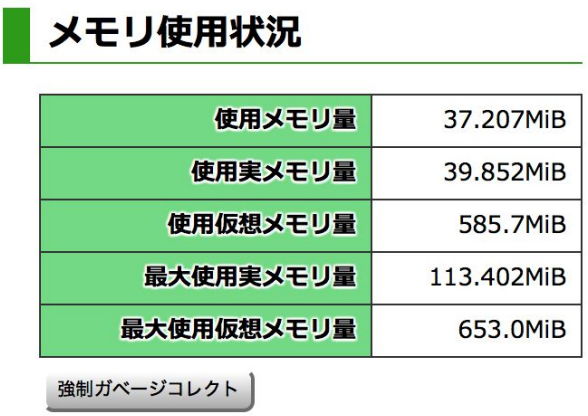
アプリケーションのバージョン番号を表示しています。

21-2. プロセス情報

アプリケーションの実行情報を表示しています。

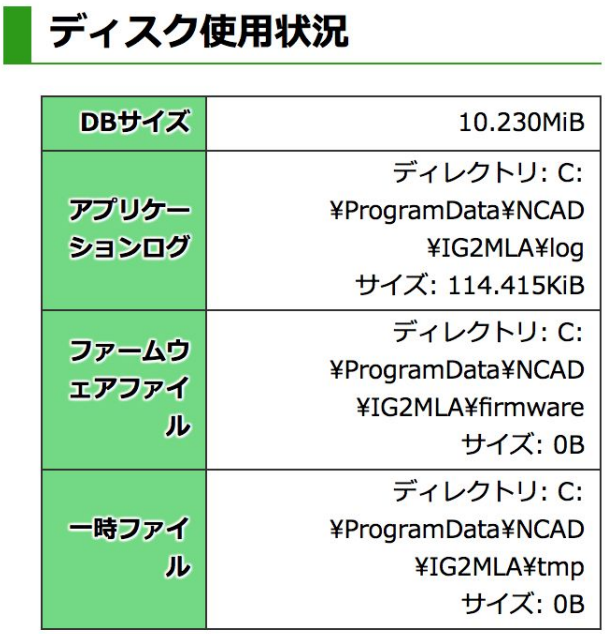
21-3. メモリ使用状況

アプリケーションのメモリ使用状況を表示しています。「**強制ガベージコレクト**」ボタンをクリックすることでガベージコレクトを強制的に実行することが可能です。



21-4. ディスク使用状況

アプリケーションで利用しているディスクの使用状況を表示しています。
DBサイズはデータベースで利用しているディスク容量です。
アプリケーションログは、アプリケーションのログが使用しているディスク容量です。
ファームウェアファイルは、アプリケーションに登録されているファームウェアファイルで使用しているディスク容量です。
一時ファイルは、アプリケーションの一時ファイルで使用しているディスク容量です。



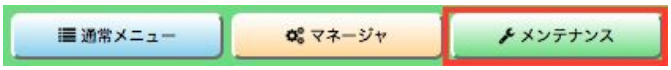
21-5. アプリケーションログ

アプリケーションのログをダウンロードや、ログ動作の変更が可能です。**ログ出力レベル**を変更することで詳細な内容まで出力することが可能ですが、ディスクの使用量は増えるため注意が必要です。**SQLログ出力**も同様で、「**はい**」内部処理のログを選択するとログを大量に出力します。

22. アプリ終了

アプリケーションの再起動、終了を管理画面から行うことができます。
※本画面は、クラウド版マネージャをご利用の場合は操作できません。

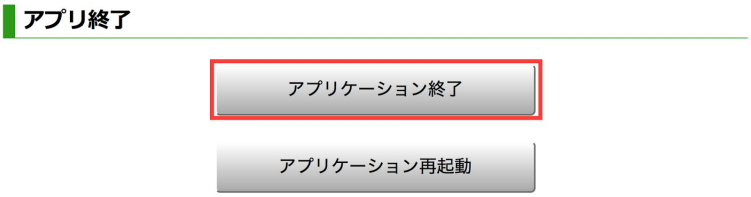
トップメニューの「**メンテナンス**」をクリックします。

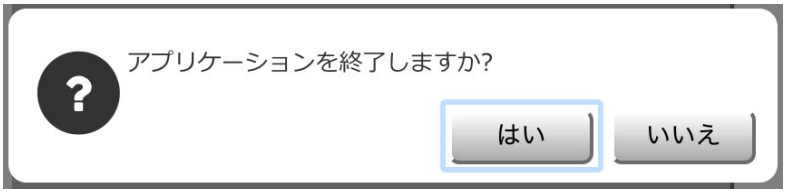


メンテナンスの「**アプリ終了**」をクリックします。

22-1. アプリケーション終了

アプリケーションの終了を行うためには、「**アプリケーション終了**」ボタンをクリックします。

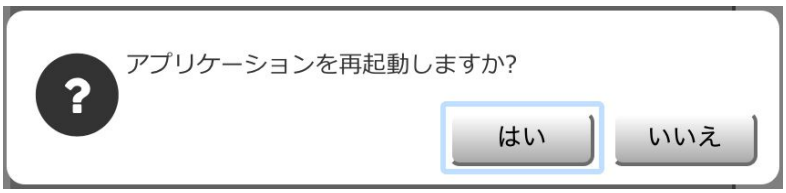




「**アプリケーション終了**」ボタンクリック後、確認ダイアログが表示されるので「**はい**」をクリックするとアプリケーションを正常終了することができます。

22-2. アプリケーション再起動

アプリケーションの再起動を行うためには、「**アプリケーション再起動**」ボタンをクリックします。



「**アプリケーション再起動**」ボタンクリック後、確認ダイアログが表示されるので「**はい**」をクリックするとアプリケーションを再起動することができます。

IntraGuardian2+ Manager Professional
Version 3.3

ユーザーマニュアル

2017年8月31日

総販売店・サポート窓口
ネットチャート株式会社
神奈川県横浜市港北区新横浜2-15-10 YS新横浜ビル8F
ig2-support@ncj.co.jp

開発元
日本シー・エー・ディー株式会社
〒161-0033 東京都新宿区下落合2-14-1 CADビル
http://www.ncad.co.jp/