IntraGuardian2+ Manager Professional

(Version 3.6.6 ～)

ユーザーマニュアル

第13版

2021年7月21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「IntraGuardian2$^+$ Manager Professional インストールガイド」を参照してください。

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

日本シー・エー・ディー株式会社（以下 「NCAD」と記載します）は、お客様（法人又は個人、商用又は非商用のいずれであるかを問わないすべての利用者様）に、本使用許諾契約 (以下「本契約」と記載します)に基づいて、不正接続検知／排除システム「IntraGuardian」シリーズ用の集中管理ソフトウェアである「IntraGuardian2+ Manager Professional」（以下「本ソフトウェア」と記載します）を使用する権利を許諾します。本ソフトウェアをインストール、複製、又は使用することによって、お客様が本契約の全てにご同意いただいたものといたします。本契約の条項に同意されない場合は、本ソフトウェアをインストール、複製、又は使用しないでください。なお、本ソフトウェアをネットワーク等を介して提供している場合、ダウンロードされる際も本契約にご同意いただく必要があります。本契約の条項に同意されない場合は、ダウンロードを中止してください。

※「IntraGuardian」は、日本シー・エー・ディー株式会社の商標です。

第１条　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、お客様において設置、使用されている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することはできません。
３．お客様は、本ソフトウェアを編集、改変、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。
４．お客様は個人的利用もしくは法人内での利用を目的としてのみ、関連資料の複製を作成できます。ただし、ハードコピーか電子文書かにかかわらず、これらをお客様の組織外に再発行したり再配布したりすることはできません。

第２条　利用者義務
お客様は、本ソフトウェアを稼働するために必要な仕様を満たしたコンピューター等のハードウェア、周辺機器、オペレーティングシステム、ネットワーク等の環境を、自らの責任と費用において確保・維持するものとします。

第３条　著作権・知的財産・商標
１．本ソフトウェアに関する著作権等の知的財産権は、NCADに帰属し、日本の著作権法その他関連して適用される法律等によって保護されています。
２．本ソフトウェアとともに提供されるドキュメント等の関連資料（以下「関連資料」と記載します）、及びサンプルコードの著作権は、NCADに帰属し、これら関連資料は日本の著作権法その他関連して適用される法律等によって保護されています。
３．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。
４．お客様は、本ソフトウェア及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することはできません。本契約に明示的に許諾されている場合に基づき本ソフトウェア及びその関連資料を複製する場合には、それらに付されている著作権表示及びその他の権利表示も同時に複製するものとします。

第４条　禁止事項
お客様は、NCADの事前の書面による承諾がない限り、次の各号に定める行為を行うことができません。
１．本契約に定める目的以外の目的で本ソフトウェアをインストールし、又は使用すること。
２．お客様がIntraGuardianの使用を取り止めた場合に、IntraGuardianの集中管理データを維持・管理する目的以外で本ソフトウェアを使用すること。
３．自身もしくは第三者を介して、本ソフトウェアの全部又は一部をリバースエンジニアリング、逆コンパイル、逆アセンブル、その他の著作権法上の複製、謄写、編集、流用、改変等の開発・製造行為を行うこと。
４．自身もしくは第三者を介して、本ソフトウェアの全部又は一部を複製・譲渡、配布、配信（ネットワーク経由であるか否かと問わず）すること。
５．自身もしくは第三者を介して、本ソフトウェアの性能を公表すること。
６．本ソフトウェアの使用権を第三者に許諾、貸与、リース、譲渡、サブライセンスすること。ただし、お客様と資本関係、取引契約のある第三者の運用を受託又は委託するための使用はこれを妨げません。

７．日本の法令等に基づく許可及びNCADの承認なく、本ソフトウェアを直接又は間接的に輸出（海外への持ち出しを含む）すること。

第５条　非保証・責任の限定
１．NCADは、本ソフトウェアに関して、その品質及び性能に関する表示、説明等に関して、いかなる明示又は黙示の保証もいたしません。
２．NCADは、お客様に対して本ソフトウェアを「現状有姿のまま」で提供するものとし、本ソフトウェアについて一切の瑕疵担保責任及び保証責任を負いません。ただし、お客様が本ソフトウェアの誤りを発見し、NCADに対して当該誤りについて書面にて通知、報告いただいた場合、修正を行うよう努力するものといたします。
３．NCADは、お客様に対して、本ソフトウェアについて誤り、エラー、動作不良もしくは他の不具合が生じないこと、第三者の権利を侵害しないこと、商品性、お客様もしくは第三者の特定の目的への適合性について一切保証いたしません。
４．NCADは、本ソフトウェアの使用又は使用不能から生じた結果について責任を負いません。
５．NCADは、逸失利益、間接損害、派生損害、データの消失やシステムの動作不良といった特別の事情から生じた損害（損害発生についてのNCADの予見の有無を問いません）等、本ソフトウェアの使用に関連して生じたお客様のいかなる損害についても賠償責任を負いません。

第６条　譲渡
１．お客様は、NCADの書面による事前の承諾なくして、本契約上の地位、並びに、本契約に基づく権利及び義務を第三者に譲渡できないものとします。
２．NCADは、事業譲渡その他事業再編のために本契約にかかる事業を他者に承継させる場合は、お客様の承諾なく、本契約上の地位及び本ソフトウェアの使用許諾権を第三者に譲渡することができるものとします。

第７条　契約開始・終了
１．本契約は、本ソフトウェアのインストール、もしくは使用を始めたとき発効し、下記により本契約が終了するまで有効であるものとします。
２．お客様は、NCADに事前に書面にて通知することにより、いつでも本契約を終了させることができます。
３．NCADは、お客様が本契約のいずれかの条項に違反した場合、お客様に対し何らの通知・催告を行うことなく直ちに本契約を終了させることができます。
４．上記３の場合、NCADは、お客様によって被った損害をお客様に請求することができます。
５．お客様は、本契約が終了したときは、直ちに本ソフトウェア及びそのすべての複製物ならびに関連資料を破棄するものとします。

第８条　権利行使
お客様は、NCADが本契約に基づき権利を行使できることを了承します。

第９条　管轄裁判所
本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。本契約の成立、効力、履行及び解釈に関しては、日本法が適用され、本規約から生じる紛争については日本国の裁判所の裁判管轄権に服するものとします。

以上

最新更新日：2018年3月9日
日本シー・エー・ディー株式会社

目次

はじめに 2

ソフトウェア使用許諾契約 3

1. 管理画面へログイン・ログアウト 9
1-1. Webブラウザを起動 9
1-2. 管理画面へログイン 9
1-3. 管理画面からログアウト 9
1-4. ログインタイムアウト 10

2. メニュー 11
2-1. 通常メニューグループ 11
2-2. マネージャグループ 11
2-2. メンテナンスグループ 11

3. セクション管理 12
3-1. セクションとは 12
3-1-1. セクションの階層構造 12
3-1-2. 登録端末 13
3-1-3. 不正端末 14
3-2. セクション登録 14
3-3. 着目セクション 16
3-3-1. 着目セクションの変更 16
3-4. セクション階層表示 17
3-5. セクション名称の変更 17
3-6. セクションの削除 18
3-7. 親セクションの変更 18
3-7-1. 親セクションの追加 18
3-7-2. 親セクションの削除 18

4. IntraGuardian本体の接続 19
4-1. IntraGuardian本体から本ソフトウェアへの接続設定 19
4-2. 接続状況の確認 19
4-3. IntraGuardian本体の割り当て 20
4-4. 割り当て中のIntraGuardian本体の設定の同期について 21

5. 監視設定 21
5-1. 監視設定における操作方法 22
5-1-1. 指定セクションに設置されていて、下位セクションには1つも設置されていないとき 22
5-1-2. 指定セクションには設置されていないが、下位セクションには設置されているとき 22
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とき 23
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とき 23
5-2. （監視設定）ネットワーク設定 24
5-3. （監視設定）基本設定 24
5-3-1. 検知・排除方式 24
5-3-2. IPアドレスの取り扱い 25
5-3-3. ホスト名検出 25
5-3-4. 巡回機能 26
5-3-5. 排除設定のカスタマイズ 26
5-4. （監視設定）メール通知設定 28
5-4-1. メール通知 28
5-4-2. IPアドレス変化 29
5-4-3. コンピュータ名変化 29
5-4-4. 稼働通知 29
5-4-5. イベント通知 30

5-5. （監視設定）SNMP設定 30
5-5-1. SNMPトラップ 30
5-5-2. 不正接続検知 31
5-5-3. 不正接続解除 32
5-5-4. IPアドレス変化 32
5-5-5. コンピュータ名変化 33
5-5-6. 稼働通知 33
5-5-7. イベント通知 33
5-6. （監視設定）高度な設定 35
5-6-1. SYSLOG設定 35
5-7. （監視設定）本体ログイン 35
5-8. （監視設定）例外アドレス 36
5-8-1. 例外IPアドレス 36
5-8-2. 例外ベンダ 36

6. 端末管理 37
6-1. 端末一覧 37
6-2. 一覧表示のカスタム 38
6-2-1. 検索条件 38
6-2-2. 表示カラム選択 38
6-2-3. スマート検知関連のカラム 39
6-3. 端末情報の新規登録（新規端末登録） 40
6-4. 端末情報の変更 42
6-5. 登録端末の削除 43
6-6. 一括セクション移動 44
6-7. 端末情報の一括削除 44

7. 不正接続一覧 45
7-1. 不正接続一覧からの端末新規登録 46
7-2. 保留時間の延長 46

8. 特別許可端末 46
8-1. 特別許可端末からの端末登録 47
8-2. 特別許可端末の端末削除 48

9. 履歴 48
9-1. 端末履歴 49
9-2. 動作履歴 50
9-3. 新しい履歴と古い履歴 51

10. マネージャ設定 52
10-1. （マネージャ設定）動作設定 52
10-2. （マネージャ設定）UI設定 53
10-3. （マネージャ設定）メール通知設定 54
10-3-1. メールの文面をカスタマイズする 55
10-4. （マネージャ設定）その他通知設定 58
10-4-1. SYSLOG設定 58
10-4-2.SNMPトラップ設定 58
10-5. （マネージャ設定）スマート検知設定 59
10-5-1. SYSLOG検知設定 59
補足：スマート検知における正規表現の使用について 60
補足：SYSLOG検知の優先順位 61
10-5-2. 振る舞い検知設定(UTM連携) 61
10-6. （マネージャ設定）バックアップ設定 62
10-7. （マネージャ設定）履歴設定 62
10-8. （マネージャ設定）新規端末登録設定 63
10-9. （マネージャ設定）登録申請設定 63

10-10. （マネージャ設定）外部端末認証設定 64
10-11. （マネージャ設定）Account@Adapter+ 連携設定 65

11. 管理者・オペレータの設定 66
11-1. 権限 66
11-2. オペレータ設定 66
11-2-1. オペレータの新規登録 67
11-2-2. オペレータ情報の変更 70
11-2-3. オペレータの削除 70
11-3. 自分の情報（個人情報）を変更する 71
11-4. セクションの管理権限 72
11-4-1. セクションの管理権限／閲覧権限を付与する 72
11-4-2. セクションの管理権限／閲覧権限を削除する 72

12. 種別管理 72
12-1. 端末種別 73
12-1-1. 端末種別の新規登録 73
12-1-2. 端末種別の変更 73
12-1-3. 端末種別の削除 74
12-2. NIC種別 74
12-2-1. NIC種別の新規登録 74
12-2-2. NIC種別の変更 74
12-2-3. NIC種別の削除 74

13. ファームウェア管理 75
13-1. ファームウェアファイルの登録 76
13-2. ファームウェアの更新予約 76

14. 登録申請機能 77
14-1. 登録申請機能とは 77
14-2. 登録申請機能の設定 77
14-2-1. （マネージャ設定）登録申請設定 77
14-2-2. 監視設定（IntraGuardian本体の設定） 80
補足：IntraGuardian本体側の設定を確認 80
14-3. 登録申請一覧 81

15. ファイル入出力 81
15-1. 端末一覧のダウンロード 82
15-2. 端末一覧のアップロード 82
補足：端末一覧のCSVファイルの仕様 83
15-3. 端末CSVファイルフォーマット 84
15-3-1.端末CSVファイルフォーマットで出力する項目 84
15-3-2.端末CSVファイルフォーマットのオプション設定 85
15-4. セクション情報のダウンロード 86
15-5. セクション情報のアップロード 86
補足：セクション情報のXMLファイルの仕様 87

16. 外部システム連携 90
16-1. 端末一覧書き出し 90
16-1-1. 指定ディレクトリへの保存 90
16-1-2. FTPへの保存 91
16-2. 端末一覧取り込み 92
16-2-1. 指定ディレクトリからの取り込み 92
16-2-2. FTPからの取り込み 93
16-3. 端末CSVフォーマット 94
16-4. セクション情報書き出し 95
16-4-1. 指定ディレクトリへの保存 95

16-4-2. FTPへの保存 96
16-5. セクション情報取り込み 97
16-5-1. 指定ディレクトリからの取り込み 97
16-5-2. FTPからの取り込み 98

17. バックアップ・復元 99
17-1. バックアップのダウンロード 99
17-2. バックアップのファイル保存 99
17-3. バックアップのFTP保存 100
17-4. 復元 100
17-4-1. ファイルをアップロードして復元 101
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 101
17-5. 自動バックアップ設定 102
17-5-1. ファイル保存方式の自動バックアップ 102
17-5-2. FTP保存方式の自動バックアップ 103

18. ライセンスコードの登録 104
18-1. 初期セットアップ時のライセンスの入力 104
18-2. 評価版として利用する 104
18-3. セットアップ後にライセンスコードを入力する 104

19. ソフトウェア更新 104
19-1. アップグレードファイルの入手 105
19-2. アップグレード 105

20. OUIコード更新 105
OUIコードとは 106
20-1. OUIコード検索 106
20-2. IEEEから最新のOUIコードをダウンロード 106
20-3. OUIコードファイルをアップロード 107

21. アプリ情報 107
21-1. バージョン情報 108
21-2. プロセス情報 108
21-3. DBアクセス状況 108
21-4. HTTPサーバ状態 108
21-5. メモリ使用状況 109
21-6. アプリケーションログ 109
21-7. ディスク使用状況 109

22. アプリ終了 111
22-1. アプリケーション終了 111
22-2. アプリケーション再起動 111

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サーバーのブラウザでも、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端末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。
※ 10081 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10081です）

IPアドレスとポート番号（URL）	http://xxx.xxx.xxx.xxx:10081/

「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。

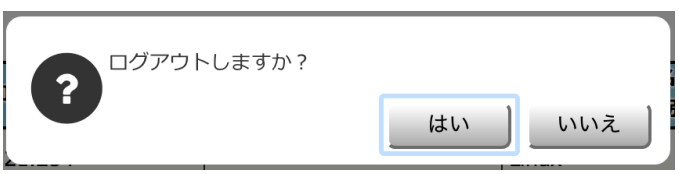
※ 現在は日本語のみ対応のため、「言語」は日本語固定です。

※「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。

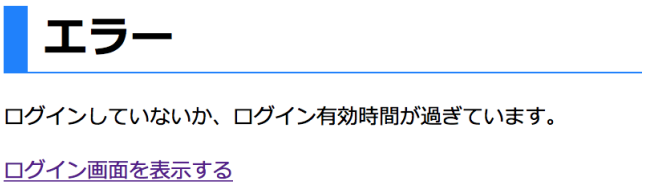
確認ダイアログが表示されますので、「**はい**」をクリックするとログアウトが完了し、ログイン画面へ遷移します。



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が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「、**【10-2.（マネージャ設定）UI設定】**」を参照してください。



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本体の設定（監視設定）を変更する、といった操作を実施することができます。

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本体の動作状況の履歴の確認、IntraGuardian2^{+} Manager Professional自身の動作設定の変更、オペレータの登録、端末種別などの項目管理、IntraGuardian本体のファームウェアのバージョンアップ、外部システムとの連携処理、といった操作を実施することができます。

マネージャグループの各種操作は、後述する**全権管理者**のみ実施することができます。

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、OUIコード（ベンダコード）のデータベースの更新、IntraGuardian本体との接続状況の確認、ライセンスの登録、本ソフトウェアのアップグレード、本ソフトウェアの再起動／終了、といった操作を実施することができます。

メンテナンスグループの各種操作は、後述する**全権管理者**のみ実施することができます。

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行います。本章ではセクションの概念について記述し、実際にセクションを作成する手順を説明します。

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。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本体を割り当てることができます。IntraGuardian本体を割り当てる場合、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。

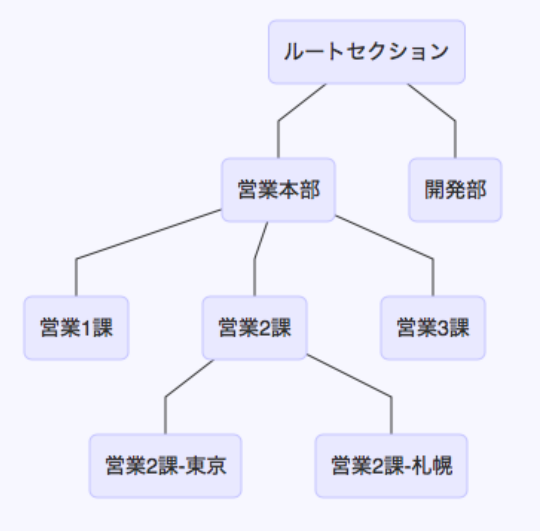
セクション1つにつき、0台または1台のIntraGuardian本体が対応することになります。1つのセクションに複数のIntraGuardian本体を割り当てることはできません。複数のIntraGuardian本体を束ねて管理したい場合、次に述べるセクションの**階層構造**を利用します。

3-1-1. セクションの階層構造

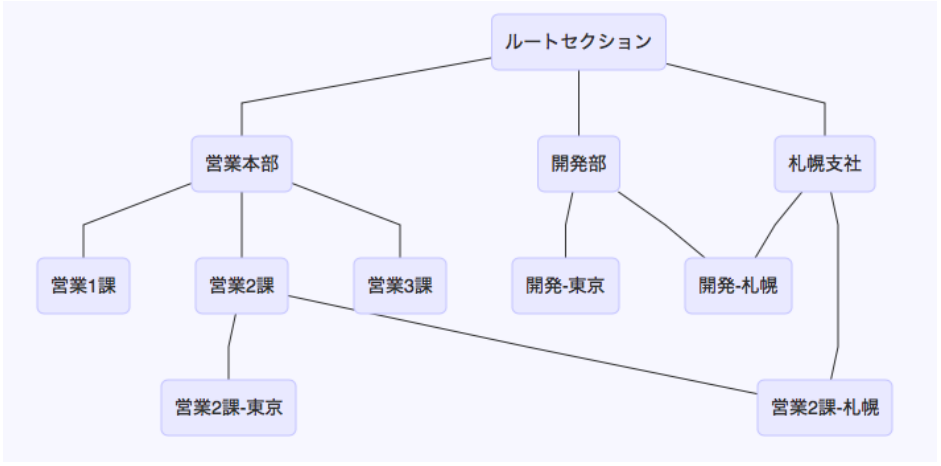
セクションは**階層構造**になっており、自身の下位セクションを任意の数だけ設置することができます。
また、セクションは必ず上位セクションを1つ以上持ちます。

例外は、全セクションの最上位となる「**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は「全体」という名前がつけられています）

右図は、セクションの階層構造の一例です。



各セクションは、上位セクションを**複数設定**することができます。ツリー構造だけでなく、下図のような複雑な構造も設定することができます。



※ ただし、自身の上位と下位が同一のセクションになるような循環関係は設定できません。

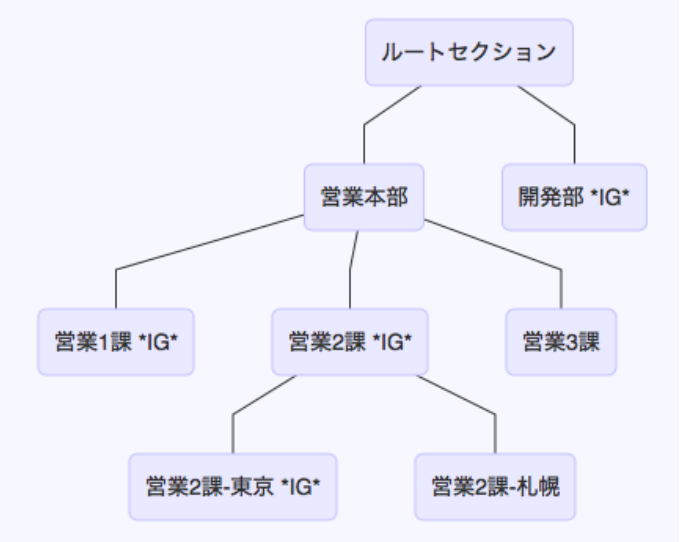
3-1-2. 登録端末

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**下位セクションに継承**されます。

例えば、右図で「営業2課」に登録された端末は、**下位セクション**である「営業2課-東京」「営業2課-札幌」にも登録されているものとして処理されます。

つまり「営業2課」に設置されたIntraGuardian本体は、「営業2課」だけでなく**上位セクション**である「営業本部」「ルートセクション」も含め、いずれかに登録されている端末が全て登録されているものとして処理されます。

（右図内の「*IG*」は、そのセクションにIntraGuardian本体が設置されていることを示しています）



同様に「営業2課-東京」に設置されたIntraGuardian本体は、「営業2課-東京」「営業2課」「営業本部」「ルートセクション」のいずれかに登録されている端末が全て登録されているものとして処理されます。

※ IntraGuardian本体のハードウェア性能の都合上、MACアドレス数ベースで40,000件を超える端末情報は送信されません。
※ 同一の端末を複数のセクションへ登録することはできません。複数のセクションで利用したい端末がある場合、それらのセクションを統括する上位セクションを作成し、そこへ端末を登録してください。

＜「営業2課」セクションでは、自身とその上位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: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	

3-1-3. 不正端末

IntraGuardian本体で検知された**不正端末**は、セクション単位で一覧することができます。不正端末は、登録端末とは逆に**上位セクション**へ向かってへ継承されます。

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課に加えて、営業2課-東京のIntraGuardian本体で検知されている不正端末も表示されます。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課に加えて、営業1課のIntraGuardian本体で検知されている不正端末も表示されます。

＜「営業本部」セクションでは、下位セクションのいずれかで検知されている不正端末も表示されます＞

3-2. セクション登録

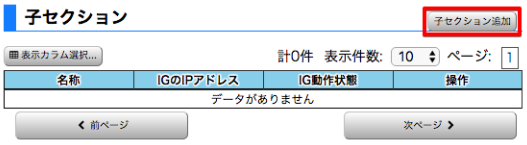
インストール直後の状態では、ルートセクション（「全体」セクション）のみ登録されています。
複数のIntraGuardian本体を管理したい場合、まずは新たな下位セクションを追加します。

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。

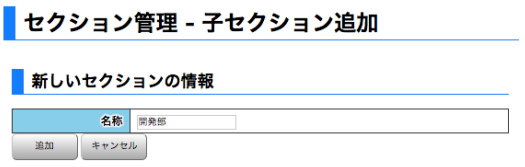
セクション追加を行うためには、セクション追加を行いたい位置から一つ上のセクション（親セクション）を指定します。
インストール直後の場合、ログイン直後に自動的に「**全体**」セクションが選択されていますので、そのまま新たな下位セクション（子セクション）を追加してください。

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うことができません。

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



※ セクションの名称は、1文字以上～99文字以下で入力してください。
※ 既存のセクション名との重複はできません。

3-3. 着目セクション

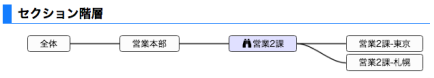
通常メニューグループの操作は全て「**現在着目しているセクション**」に対して実行されます。現在着目しているセクションは、**ブラウザの左上**に表示されています。

3-3-1. 着目セクションの変更

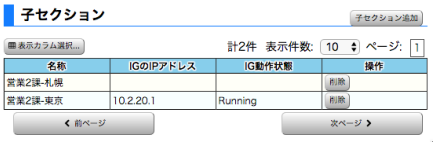
着目セクションを変更する方法は3つあります。見やすい方法を利用してください。

1. **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、「**セクションの選択**」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。

2. **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、全てのセクション名が表示されず選択できないことがあります。



3. **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、子セクションの一覧表の行をクリックしても切り替わります。子セクションが多数ある場合、ページの切替などを行って、切り替えたいセクション名を表示させてからクリックしてください。



3-4. セクション階層表示

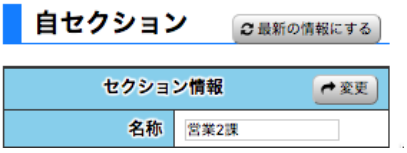
セクション階層の図は、利用中の環境で見やすくなるように調整することができます。

セクション階層の「**表示設定**」をクリックすると、右図の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。この設定はオペレータ毎に保存されます。

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のみ表示するため、セクションの階層が複雑なときに見やすくなります 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、全てを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を指定します
上位セクション段数	現在セクションから上位何段のセクションまで表示するか指定します **※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を指定します
セクション名余白	セクション名とその周りの線との距離を指定します
文字サイズ	セクション名の表示に用いる文字サイズを指定します

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。
文字数を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。

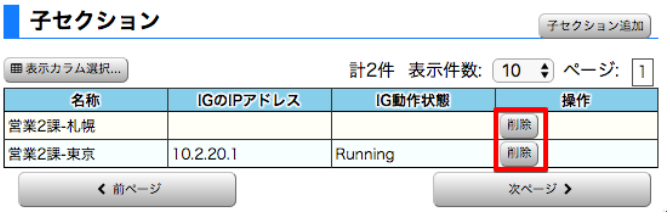


名称を変更後、「**変更**」ボタンをクリックで完了です。

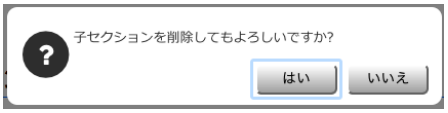
※ セクションの名称は、1文字以上～99文字以下で入力してください。
※ 既存のセクション名との重複はできません。

3-6. セクションの削除

セクションの削除は、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。

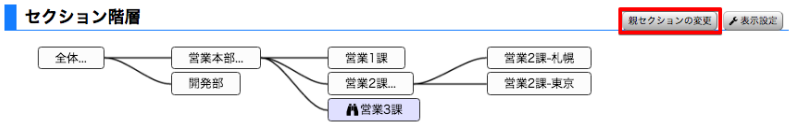


確認画面が表示されるので、「**はい**」を選択すると削除完了です。



3-7. 親セクションの変更

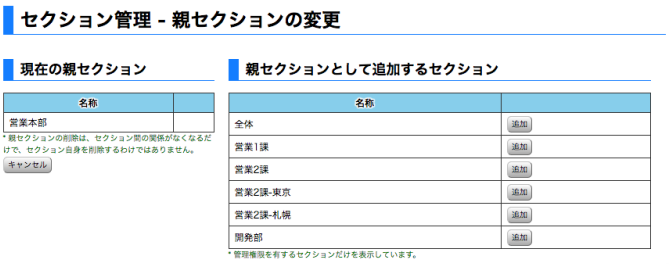
親セクションを変更する場合、変更したいセクションのセクション管理画面にある「**親セクションの変更**」ボタンをクリックします。



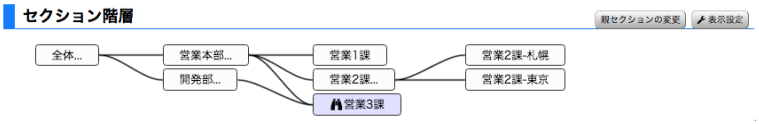
3-7-1. 親セクションの追加

親セクションを追加する場合、「**親セクションとして追加するセクション**」一覧の、該当セクション名の右にある「**追加**」ボタンをクリックします。

※関係が重複する場合、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替が行われます。



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。



3-7-2. 親セクションの削除

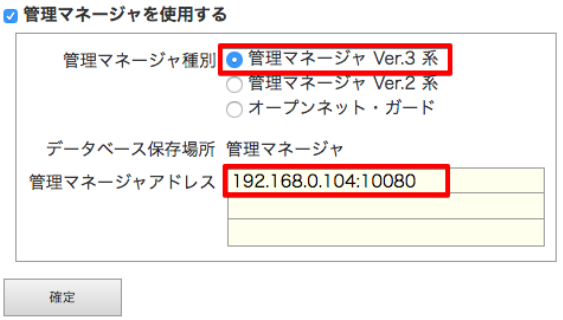
親セクションを削除する場合、「**現在の親セクション**」一覧の、該当セクション名の右にある「**削除**」ボタンをクリックします。

4. IntraGuardian本体の接続

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**IntraGuardian本体との接続**を行います。
IntraGuardian本体の管理画面から本ソフトウェアへ接続するための設定を行った後、次に本ソフトウェアの管理画面を使用してIntraGuardian本体の接続を受け付ける設定を行います。

4-1. IntraGuardian本体から本ソフトウェアへの接続設定

※ IntraGuardian本体のファームウェアがバージョン3未満の場合、本ソフトウェアとの通信をサポートしておりません。



1. IntraGuardian本体の管理画面にブラウザでアクセスし、ログインします。

2. **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。

3. 「**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。

   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。

4. 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. 接続状況の確認

IntraGuardian本体の設定を終えると、IntraGuardian本体は本ソフトウェアへ接続を試み始めます。
IntraGuardian本体からの接続要求が本ソフトウェア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**」画面で確認可能です。

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本体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本体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本体からの接続要求が本ソフトウェアへ届いていない（上記一覧に表示されない）場合、次の点を確認してください。

1. IntraGuardian本体は本ソフトウェア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アドレスは正しく入力されていますか？
2. IntraGuardian本体の設置設定は正しく設定されていますか？
   - 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本体から本ソフトウェアまで、ネットワーク的に正しく接続されていますか？
   - IntraGuardian本体は本ソフトウェアの17777番ポートにTCP接続をしますが、このソケットを途中で遮断するようなネットワーク機器などは存在しませんか？
4. 本ソフトウェアを稼働しているWindows上でセキュリティ監視ソフトが動作していませんか？
   - 本ソフトウェアは17777番ポートのTCP通信を受信しますが、これをブロックするような設定、又はソフトウェアが動作していませんか？
5. 該当のIntraGuardian本体は既に本ソフトウェアで登録済（割り当て済）ではありませんか？
   - 「**接続中のみ**」のラジオボタンをクリックすると該当のIntraGuardian本体が表示されます。

4-3. IntraGuardian本体の割り当て

続いて、不正端末の検知／排除の動作を開始するために、IntraGuardian本体をセクションへ割り当てます。

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。

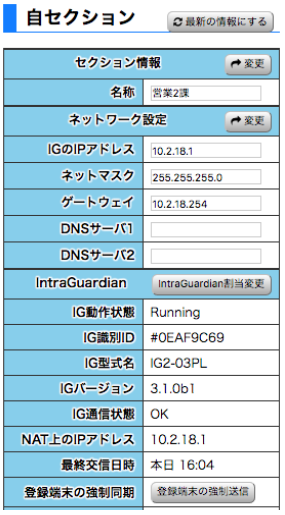
次に、画面の左側に表示されている「**自セクション**」の「**IntraGuarian新規割当**」ボタンをクリックします。

※ 既に本セクションへIntraGuardian本体が割り当たっている場合、ボタン名が「IntraGuardian割当変更」に変化します。

画面が「**セクション管理 - IntraGuardian割り当て**」に切り変わり、現在接続要求中のIntraGuardian本体が一覧に表示されます。
IPアドレスから登録するIntraGuardian本体を判別し、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、本ソフトウェアから見たIntraGuardian本体のIPアドレスです。
通常はIntraGuardian本体のIPアドレスと同一のアドレスが表示されますが、IntraGuardian本体と本ソフトウェアとの間にIPアドレス変換を伴うルータなどが入っている場合、異なるアドレスが表示されていることがあります。
また、IntraGuardian本体が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用し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。

割り当てが完了すると、「**自セクション**」欄にIntraGuardian本体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**」をクリックします。

4-4. 割り当て中のIntraGuardian本体の設定の同期について

セクションに割り当てられたIntraGuardian本体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本体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、削除および編集を行うことはできません。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本体が本ソフトウェア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本体の設定内容は、次の場合に本ソフトウェアからIntraGuardian本体へ送信されます。

- IntraGuardian本体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本体の設定（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

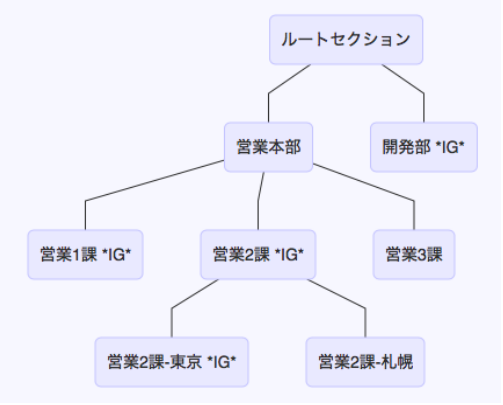
通常メニューの**監視設定**画面を使用すると、指定セクションとその下位セクションに設置されているIntraGuardian本体の設定をまとめて変更できます。

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本体の設定**と、**指定セクションの下位セクションに設置されているIntraGuardian本体の全ての設定**をまとめて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通りに変化します。

本節では4通りの状態を、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本体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、下位セクションには1つも設置されていないとき

右図は、**指定セクションにIntraGuardian本体が設置されていて、指定セクションの下位セクションにはIntraGuardian本体が設置されていない**ときの表示です。
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本体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、下位セクションには設置されているとき

右図は、**指定されたセクションにはIntraGuardian本体が設置されておらず、指定セクションの下位セクションのいずれかにIntraGuardian本体が設置されている**ときの表示です。
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下位セクションに設置されているIntraGuardian本体の全てに適用されます。
指定されたセクション以下に複数のIntraGuardian本体が存在した場合、全てのIntraGuardian本体の設定が更新されますので、注意してください。

斜めの鎖のマークは、対象のIntraGuardian本体の全台で設定が同一になっていることを示しています。設定が全台で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。

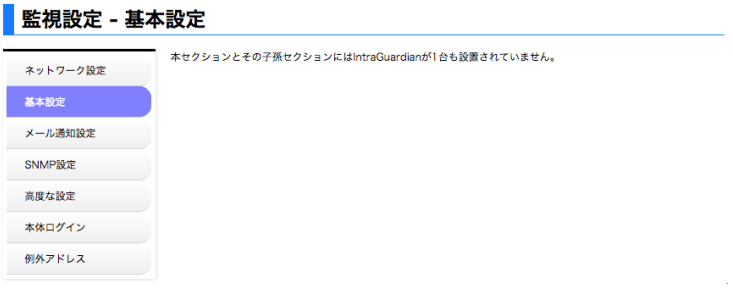
5-1-3. 指定されたセクションに設置されていて、子孫セクションにも設置されているとき

右図は、**指定セクションにIntraGuardian本体が設置されていて、指定セクションの下位セクションのいずれかにもIntraGuardian本体が設置されている**ときの表示です。
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セクションのIntraGuardian本体のみ設定が変更されます。
「**全体更新**」を選択・クリックすると指定セクションの他、下位セクションに設置されたIntraGuardian本体の設定も全て変更されます。

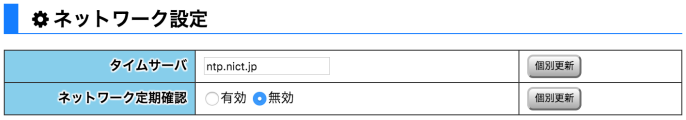
斜めの鎖のマークは、対象となるIntraGuardian本体の全台で設定が同一になっていることを示しています。設定が全台で同じになっていない項目については、切れた鎖のマークが表示されます。

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とき



右図は、**指定セクションにも、その下位セクションにもIntraGuardian本体が全く設置されていない**ときの表示です。
前述のセクション構成の例では、「営業3課」「営業2課-札幌」がこのケースに当てはまります。
この場合、「**監視設定**」画面で操作することはできません。

5-2. （監視設定）ネットワーク設定



IntraGuardian本体のタイムサーバ、及びネットワーク定期確認を設定することができます。

※ IntraGuardianが用いるIPアドレスなど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。

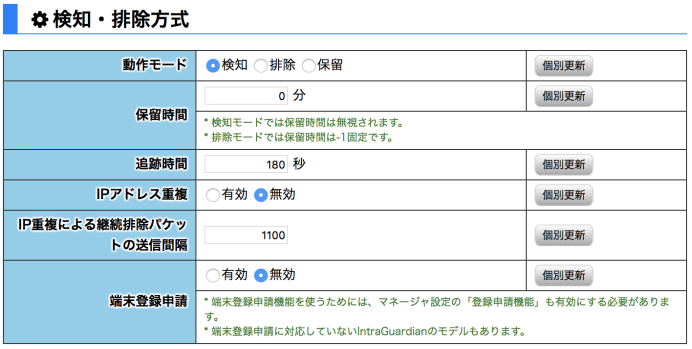
タイムサーバ	時間同期するサーバを指定します
ネットワーク定期確認	有効に設定すると、ゲートウェイアドレスに定期的にpingを送信し応答がなければネットワークインターフェースを再起動します

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-3. （監視設定）基本設定

IntraGuardian本体の基本動作設定を更新できます。

5-3-1. 検知・排除方式

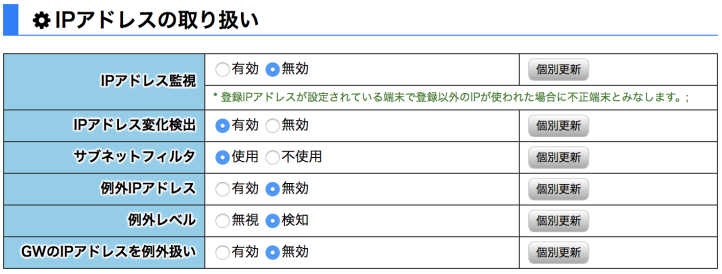


IntraGuardian本体の検知・排除の動作を設定することができます。

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
不正端末追跡時間	不正接続端末がLAN上で現在接続状態になっているかを判定するための制限時間です
登録済み端末追跡時間	登録済み端末がLAN上で現在接続状態になっているかを判定するための制限時間です
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
IP重複による継続排除パケットの送信間隔	IP重複による継続排除パケットの送信間隔を設定します
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**

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

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
IPアドレス変化検出	IPアドレス変化検出を有効にするとIPアドレス変化を検出した場合にメールで通知します
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指定します
例外レベル	例外IPアドレスを有効にした実際に場合に、検知時に自動登録イベントの通知を行うか無視するか設定します
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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-3-3. ホスト名検出

IntraGuardian本体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
IPv6機能を有効にする	IPv6機能の有効／無効を切り替えます

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-3-4. 巡回機能

IntraGuardian本体が、ネットワークを巡回監視するときのパラメータを設定することができます。

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IPアドレス数の合計値は65535個までです**

5-3-5. 排除設定のカスタマイズ

排除時のMACアドレスや、排除パケットの送信回数、送信間隔など、排除パケットの内容を細かく指定することができます。

※ 特別に設定を変更しなければならない状況を除いて、排除設定のカスタマイズを有効にしないでください。

排除設定のカスタマイズ	排除設定のカスタマイズ機能を「**有効**」にするか選択します。「**無効**」の場合、以下の設定項目は無視されます
不正端末宛ての排除パケット送信先MACアドレス(Ether Frame)	不正端末宛てのEthernetの排除パケットにおいて、送信先MACアドレスを「**不正端末のMACアドレス**」のみにするか「**ブロードキャストアドレス**」にするか選択します デフォルト値＝不正端末のMACアドレス
不正端末宛ての排除パケットの送信元MACアドレス(ARP Packet)	不正端末宛てのARPの排除パケットにおいて、送信元MACアドレスに「**不正端末のMACアドレス**」を使用するか「**IntraGuardian本体のMACアドレス**」を使用するか選択します。 デフォルト値＝不正端末のMACアドレス **※端末登録申請が有効になっている場合、この設定は無視されます**
不正端末宛ての排除パケットの送信先MACアドレス(ARP Packet)	不正端末宛てのARPの排除パケットにおいて、送信先MACアドレスを「**不正端末のMACアドレス**」のみにするか「**ブロードキャストアドレス**」にするか選択します デフォルト値＝不正端末のMACアドレス
不正接続端末への即時応答を有効にする	不正接続端末に対する即時応答を有効にするかどうか選択します
不正接続端末への即時応答回数	不正接続端末に対する即時応答を何回行うか設定します デフォルト値＝2
不正接続端末への即時応答間隔	不正接続端末に対する即時応答を複数回行う場合に、即時応答の間隔を何ミリ秒空けるか設定します デフォルト値＝20
不正端末から不正端末への通信の継続妨害を有効にする	不正端末から、別の不正端末への通信に対して継続的な妨害を行うかどうか設定します
不正->不正への継続妨害間隔	不正端末から、別の不正端末への通信に対して継続的な妨害を行うとき、妨害の間隔を何ミリ秒空けるか設定します デフォルト値＝1100
不正端末から登録端末への通信の継続妨害を有効にする	不正端末から登録端末への通信に対して、継続的な妨害を行うかどうか設定します
不正->登録への継続妨害間隔	不正端末から登録端末への通信に対して継続的な妨害を行うとき、妨害の間隔を何ミリ秒空けるか設定します デフォルト値＝1100
正規端末宛ての排除パケットの送信元MACアドレス(ARP Packet)	正規端末宛てのARPの排除パケットにおいて、送信元MACアドレスに「**正規端末のMACアドレス**」を使用するか「**IntraGuardian本体のMACアドレス**」を使用するか選択します。端末登録申請が無効のときにIntraGuardian本体のMACアドレスを選択した場合、ダミーアドレスが使用されます デフォルト値＝正規端末のMACアドレス
正規端末宛ての排除パケットの送信先MACアドレス(ARP Packet)	正規端末宛てのARPの排除パケットにおいて、送信先MACアドレスを「**正規端末のMACアドレス**」のみにするか「**ブロードキャストアドレス**」にするか選択します。端末登録申請が無効のときにIntraGuardian本体のMACアドレスを選択した場合、ダミーアドレスが使用されます デフォルト値＝正規端末のMACアドレス
登録済み端末への即時応答を有効にする	登録済み端末に対する即時応答を有効にするかどうか選択します
登録済み端末への即時応答回数	登録済み端末に対する即時応答を何回行うか設定します デフォルト値＝2
登録済み接続端末への即時応答間隔	登録済み端末に対する即時応答を行うとき、即時応答の間隔を何ミリ秒空けるか設定します デフォルト値＝1100
登録端末から不正端末への通信の継続妨害を有効にする	登録端末から不正端末への通信に対して継続的な妨害を行うかどうか設定します
登録->不正への継続妨害間隔	登録端末から不正端末への通信に対して継続的な妨害を行うとき、妨害の間隔を何ミリ秒空けるか設定します デフォルト値＝1100

5-4. （監視設定）メール通知設定

IntraGuardian本体で利用可能なメール通知の送信設定を行うことができます。

※ 本項目の設定はIntraGuardian本体から送信するメールの設定です。本ソフトウェアからの通知設定とは異なる機能ですので、注意してください。

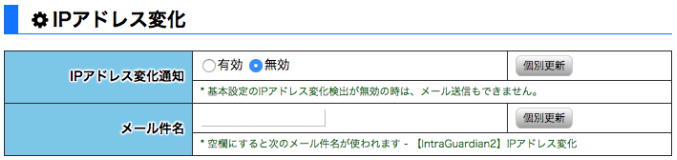
5-4-1. メール通知

IntraGuardian本体からメール通知を行う際のパラメータを設定することができます。

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（通常は25です）
送信元	通知メールを送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）の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（通常は110です）
アカウント	認証で使用するユーザーアカウントを設定します
パスワード	認証で使用するパスワードを設定します
メール集約時間	本項目の時間内にメール送信イベントが発生した場合、1通に集約されます
再送待ち時間	メール送信に失敗したとき、再送までの待ち時間を設定します
最大再送回数	メール送信に失敗したとき、再送する回数を設定します

※ 設定項目の詳細は、IntraGuardianの本体スタートアップガイドを参照してください。

5-4-2. IPアドレス変化

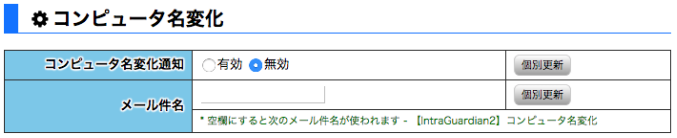


検知した端末が使用しているIPアドレスが変化したとき、メール通知を発行する機能について設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-4-3. コンピュータ名変化

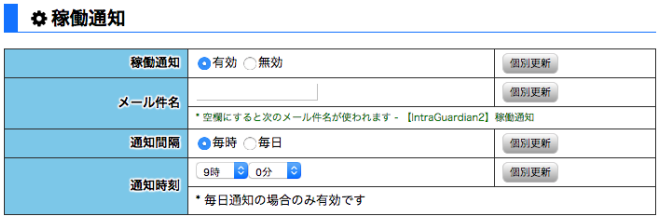


検知した端末が使っているホスト名が変化したとき、メール通知を発行する機能を設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-4-4. 稼働通知

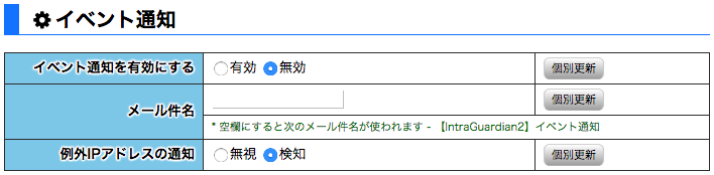


IntraGuardian本体が動作していることを、定期的にメール通知する機能を設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

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を設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-5. （監視設定）SNMP設定

5-5-1. SNMPトラップ

SNMPトラップを利用した通知を設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-5-2. 不正接続検知

不正接続を検知したときの、SNMPトラップについて設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-5-3. 不正接続解除

不正端末を登録することにより、不正接続状態が解除されたことを通知するSNMPトラップを設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-5-4. IPアドレス変化

IPアドレスが変化したときのSNMPトラップを設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-5-5. コンピュータ名変化

コンピュータ名が変化したときのSNMPトラップを設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

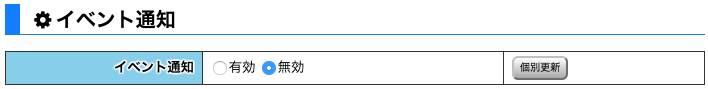
5-5-6. 稼働通知

IntraGuardian本体が動作していることを、定期的に通知するSNMPトラップを設定することができます。

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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

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トラップを設定することができます。

イベント通知	イベント通知を有効／無効化します

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-6. （監視設定）高度な設定

5-6-1. SYSLOG設定

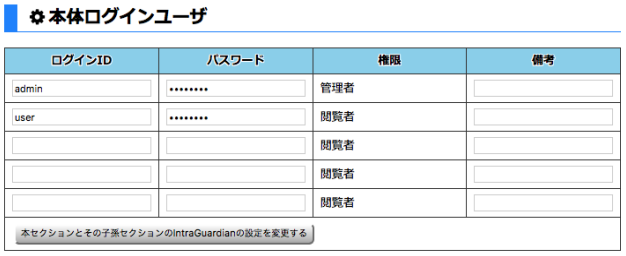
IntraGuardianが発行するSYSLOGを設定することができます。

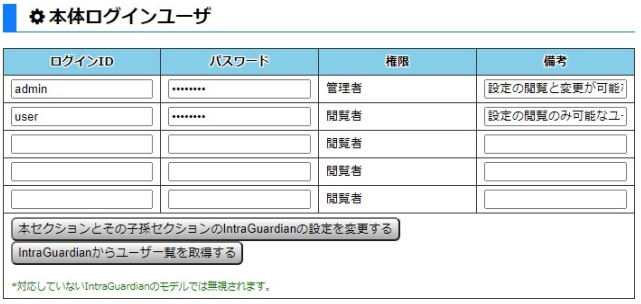
SYSLOGを利用する	SYSLOGの利用を有効／無効化します
SYSLOGサーバ	SYSLOGサーバのIPアドレスを指定します
ログレベル	ログレベルを指定します

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-7. （監視設定）本体ログイン

IntraGuardian本体のUIへログインするときに利用するIDとパスワードを設定することができます。



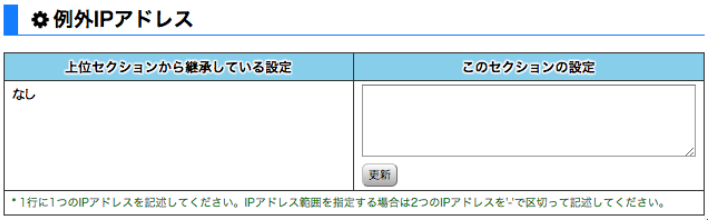


ログインID	ログインIDを設定します
パスワード	各ログインIDに対応するログインパスワードを設定します
権限	権限を指定します
備考	備考を記入できます

※ 「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本体の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、選択セクションとその子孫セクションに設定されているIntraGuardian本体の設定が変更されます。
※ 「IntraGuardianからユーザ一覧を取得する」をクリックすると、IntraGuardian本体からユーザ情報を取得します。
※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

5-8. （監視設定）例外アドレス

5-8-1. 例外IPアドレス

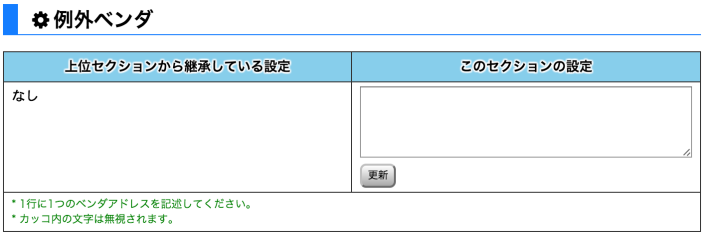


検知／排除の対象としないIPアドレスを設定することができます。
本項目の設定は、上位のセクションの設定が下位のセクションに継承されます。従って、「上位セクションから継承されている設定」と「このセクションの設定」を合わせたものが IntraGuardian本体に設定されます。

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IPアドレス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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

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されます。従って、「上位セクションから継承されている設定」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

※ 設定項目の詳細は、IntraGuardian本体のスタートアップガイドを参照してください。

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されます。（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

端末情報を一覧で確認できます。

通常は「本セクションで有効な端末」を表示して使用しますが、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た端末のみ」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。

この画面では、右上のボタンを使って次の操作を行うことができます。

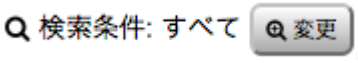
最新の情報にする	ブラウザに最新の情報をリロードします **※ IntraGuardian本体との同期処理を開始するボタンではありません**
新規端末登録	新規に端末を登録するページに遷移します
一括セクション移動	表示されている端末を一括して別のセクションに移動するための子ウィンドウを表示します
一括削除	表示されている端末を一括削除します
CSVダウンロード	表示されている端末を一括してCSVファイルとしてダウンロードします

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。

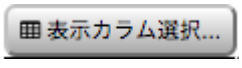
※検索条件や表示件数などの表示設定内容はオペレータ毎に保存され、ログアウト後も記憶されます。

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で表示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、次回ログイン時も反映されます。

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マイズ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／降順の変更を行うことができます。

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**」になっている全ての表示カラム同士の相対指定になります。例えば、表示カラムが4個のときに3個を100%指定、残りの1個を200%指定した場合、残りの1個は他の3個の2倍の幅で全幅に収まるよう表示されます。また、３個を50%指定、残りの1個を100%指定した場合も相対指定になるため、残りの1個は他の3個の2倍の幅で全幅に収まるよう表示されます。＋記号と−記号はそれぞれ、10%づつ拡幅と減幅を行います。

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個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。

6-2-3. スマート検知関連のカラム

以下は、スマート検知の状態の確認とそれに対する操作を行うためのカラムです。
スマート検知機能を使用する場合、これらのカラムを表示しておいてください。

スマート検知	「なし」「SYSLOG検知」「振る舞い検知」「手動検知」の4個の状態を持ちます SYSLOG検知と振る舞い検知は複合することがあります
操作	スマート検知が「なし」の場合、検知ボタンを押下することで該当の登録済端末を検知（排除）状態にすることができます。 スマート検知が「SYSLOG検知」「振る舞い検知」「手動検知」の場合、解除ボタンをクリックすることで該当の登録済み端末の検知（排除）状態を解除することができます

検知なしの状態

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	スマート検知	操作
全体	デモ用端末	Windows				11:22:33:44:55:66 Unknown	192.168.100.100	なし	検知

手動検知の状態

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	スマート検知	操作
全体	デモ用端末	Windows				11:22:33:44:55:66 Unknown	192.168.100.100	手動検知	解除

SYSLOG検知の状態

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	スマート検知	操作
全体	デモ用端末	Windows				11:22:33:44:55:66 Unknown	192.168.100.100	シスログ検知	解除

振る舞い検知の状態

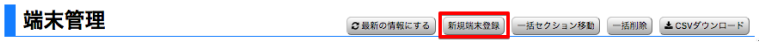
登録セクション	端末名	端末種別	有効期限	ホスト名 ワークグループ	初検知日時 確認日時	MACアドレス ベンダ	現在IPアドレス 登録IPアドレス	スマート検知	操作
全体	デモ用端末	Windows				11:22:33:44:55:66 Unknown	192.168.100.100	振る舞い検知	解除

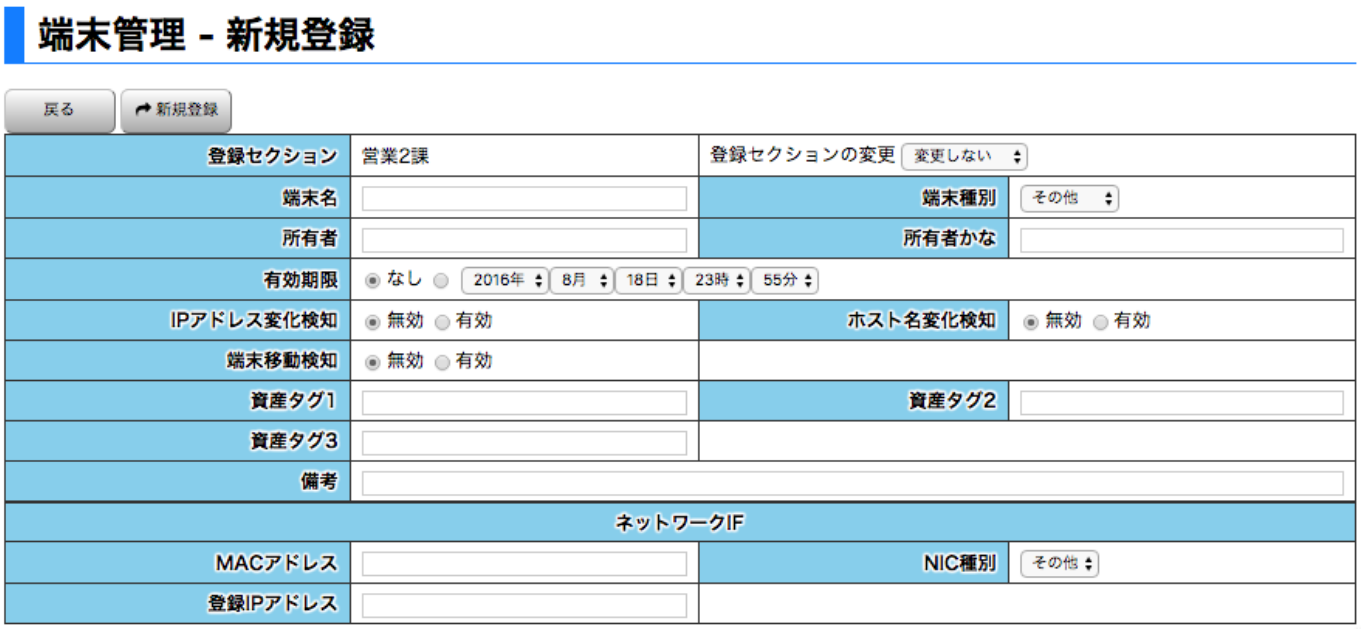
SYSLOG検知と振る舞い検知が複合した状態

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	スマート検知	操作
全体	デモ用端末	Windows				11:22:33:44:55:66 Unknown	192.168.100.100	シスログ検知,振る舞い検知	解除

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。





入力可能な項目は以下の通りです。

登録セクション	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	現在着目中のセクション以外のセクションへ端末を登録するときに選択します
端末名	端末につける名称を設定します 空欄のまま端末を登録すると、自動的に[セクション名]＋[付番]で名前が設定されます **※ 同一のセクション内で重複させ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	この端末の所有者のふりがなを入力することができます
有効期限	この端末がネットワークに接続できる期日を設定することができます
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どうか選択します
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どうか選択します
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どうか選択します
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アドレスです **※全てのオクテットが「00」又は「FF」の場合、登録できません**
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／排除動作に影響はありません。管理をしやすくするための情報です
登録IPアドレス	この端末が使用する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。

「**資産タグ1**」「**資産タグ2**」「**資産タグ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

端末の情報を変更することができます。
編集する端末の行をクリックします。すると、次のような登録変更画面が表示されます。

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			

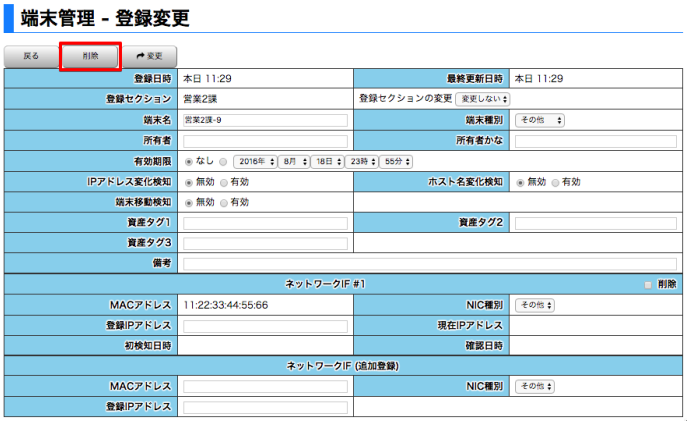
各項目の説明は「**6-3. 端末情報の新規登録（新規端末登録）**」を参照してください。
変更後、「**更新**」ボタンをクリックし変更完了です。

6-5. 登録端末の削除

　登録端末の削除を行うことができます。
削除する端末の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	

登録変更の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。

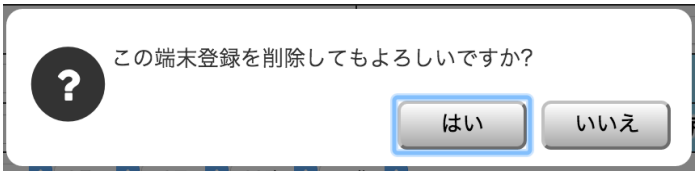


端末管理 - 登録変更

戻る　削除　変更

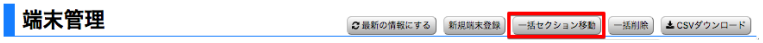
登録日時	本日 11:29	最終更新日時	本日 11:29
登録セクション	営業2課	登録セクションの変更	変更しない
端末名	営業2課-9	端末種別	その他
所有者		所有者かな	
有効期限	なし 2016年 8月 18日 23時 55分		
IPアドレス変化検知	無効 有効	ホスト名変化検知	無効 有効
端末移動検知	無効 有効		
資産タグ1		資産タグ2	
資産タグ3			
備考			
ネットワークIF #1			削除
MACアドレス	11:22:33:44:55:66	NIC種別	その他
登録IPアドレス		現在IPアドレス	
初検知日時		確認日時	
ネットワークIF (追加登録)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

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



6-6. 一括セクション移動

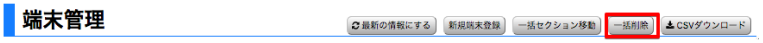
検索条件に合致する全ての端末を一括して他のセクションへ移動することができます。



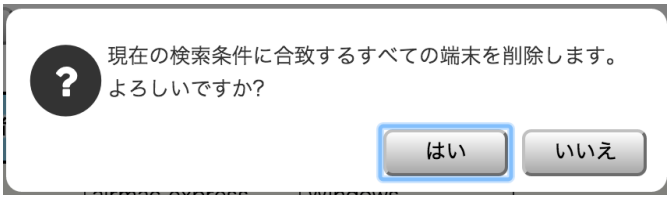
「**一括セクション移動**」ボタンをクリックすると右図のウィンドウが表示されますので、移動先セクションを選択してから「**実行**」ボタンをクリックすると、一括でセクションの移動が実行されます。

6-7. 端末情報の一括削除

検索条件に合致する全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本体が検知している不正接続端末が表示されます。

この画面では、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開始するボタンではありません**
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。

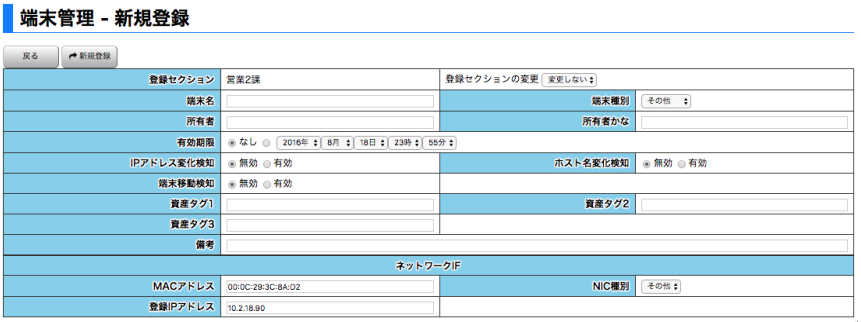
セクション	MACアドレス ベンダ	IPアドレス 別IPアドレス	ホスト名 ワークグループ	OS名 OS種別	検知日時 確認日時	保留時間	状態
営業2課	00:0C:29:3C:8A:D2 VMware	10.2.18.90 fe80::20c:29ff:fe3c:8ad2	TEST-PCSIMULATO IT		本日 13:15 本日 13:23	80	保留中
営業2課-東京	0C:AD:0A:02:16:48 Unknown	10.2.22.72			本日 13:17 本日 13:23	0	排除中

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、該当端末を正規の端末として登録するかを選択できます。「**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本体が無い場合、上記処理選択画面は表示されず直接新規登録画面が表示されます。

新規登録の画面は「**6-3. 端末情報の新規登録（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の状態になっています。



登録が完了すると、不正接続一覧画面上では**取り消し線**が表示されます。次にIntraGuardian本体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注意してください。
なお、IntraGuardian本体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本体が無い場合、上記処理選択画面は表示されないため、保留時間延長操作はできません。

8. 特別許可端末

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することができます。
本画面で表示される端末は以下のとおりです。

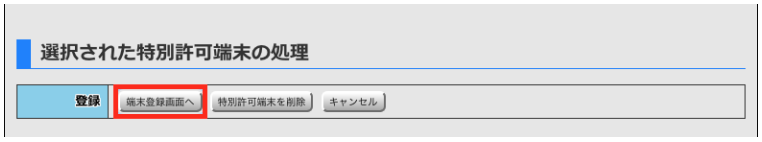
- 「**例外IPアドレス**」で許可された端末
- 「**例外ベンダ**」で許可された端末
- 「**外部端末認証**」で許可された端末
- 「**Account@Adapter+連携**」で許可された端末

8-1. 特別許可端末からの端末登録

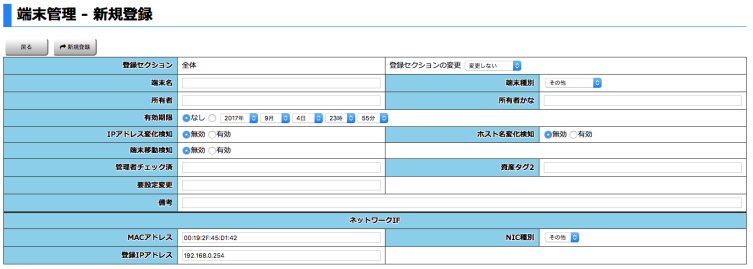
特別許可された端末は、下図のように一覧で表示されます。
一覧から端末登録を行うには、該当の端末を選択します。

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

「端末登録画面へ」ボタンをクリックします。



新規登録の画面は「**6-3. 端末情報の新規登録（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。

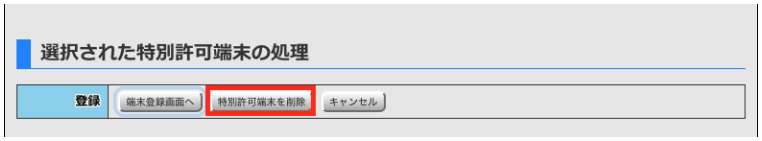


8-2. 特別許可端末の端末削除

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。
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。

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

「**特別許可端末を削除**」ボタンをクリックすると削除が完了します。



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本体の死活状態変化の履歴などです。通常の運用では、端末履歴を主に利用します。

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毎に表示します。

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	利用申請機能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本体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のみ確認することができます。

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

記録される履歴は、以下の4個に分類され保存されています。検索条件を使用して、以下の分類で絞り込んで表示することもできます。

IG関連	IntraGuardian本体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本体に関連するイベントは以下の種類があります。

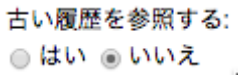
< IG関連イベント一覧 >

リンクアップ	IntraGuardian本体がリンクアップした
エンジン再起動	IntraGuardian本体の検知・排除システムが再起動した
エンジン停止	IntraGuardian本体の検知・排除システムが停止した
マネージャ接続開始	IntraGuardian本体が本ソフトウェアと接続開始した
マネージャ接続切断	IntraGuardian本体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いくため、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**」に分けて保存しています。「**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、高速に動作します。

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ます。この履歴の整理作業は1日1回、深夜に実行されます。

上で述べた、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ので、利用中の環境に合わせて調整してください。

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
- スマート検知設定
- 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本体との通信設定を行うことができます。

IGステータス確認間隔	IntraGuardian本体と通信を行う間隔（ポーリング間隔）を設定します 環境に応じて10～180秒程度で設定してください
検知情報収集間隔	IntraGuardian本体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 **※ 本項目は、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秒と設定した場合、実際の検知情報収集間隔は20秒で実行されます**
登録端末強制同期	登録端末の情報を強制的に同期します。「**はい**」にすると「**登録端末強制同期時刻**」が表示されますので時刻を設定します **登録端末強制同期** はい いいえ 更新 **登録端末強制同期時刻** 毎日 2時 20分 更新 **※ IntraGuardian本体と通信が成立しているときは、登録端末の情報に差分が生じると自動的に同期するため、通常は「いいえ」で問題ありません**
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します。「**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ので、時刻と判断日数を指定します **未使用端末自動削除** はい いいえ 更新 **未使用端末自動削除時刻** 毎日 2時 0分 更新 **未使用端末と判断する日数** 180 日 更新

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画面上の動作を設定することができます。

ログインタイムアウト	操作を行っていないとき、自動ログアウトまでのタイムアウトを設定できます
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 本欄へ入力すると、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全て入力した文字列に置換されます
資産タグ2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 本欄へ入力すると、本ソフトウェアのUI上で「**資産タグ2**」と表示している部分が全て入力した文字列に置換されます
資産タグ3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 本欄へ入力すると、本ソフトウェアのUI上で「**資産タグ3**」と表示している部分が全て入力した文字列に置換されます

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 通常は25番、又は587番です
SSL利用	SMTPサーバがSTARTTLS対応の場合「**STARTTLS 対応**」を選択します SMTPサーバがSTARTTLS対応しているが正規のサーバ証明書を持っていない場合「**STARTTLS（証明書無視）**」を選択します
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ます SMTPAUTH認証の場合は、ユーザ名とパスワードを入力します
メール集約時間	短時間で連続してメール通知が行われないよう、イベントが発生しても本項目の時間を待ってから送信します。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	全イベントを一通のメールに集約する場合は「**全イベントを集約**」を選択します 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**」を選択します
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なる場合、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**」を選択します
文面カスタマイズ	**※ 詳細は次項の「10-3-1. メールの文面をカスタマイズする」を参照してください**
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利用します

10-3-1. メールの文面をカスタマイズする

メールの文面をカスタマイズすることができます。
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。

メール本文の文字列には**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。使用できる変数と置き換え対象は次の通りです。

変数	置き換え対象
{section}	セクション名
{oldsection}	以前のセクション名
{hostname}	ホスト名
{oldhostname}	以前のホスト名
{hostos}	OS名
{hosttype}	TYPE名
{workgroup}	ワークグループ名
{lladdr}	イベントが発生したときのMACアドレス
{ipaddr}	イベントが発生したときのIPアドレス
{orgipaddr}	登録されているIPアドレス
{expiretime}	有効期限
{reservetime}	保留時間
{oldipaddr}	IPアドレス変化時の変化前IPアドレス
{note}	利用申請時の備考
{igipaddr}	IntraGuardian本体のIPアドレス

カスタマイズ項目は以下のとおりです。

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 ※ 変数を含めることはできません
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 ※ 変数を含めることはできません
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
登録端末検出系イベントグループ	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
	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本体の電源がONになったときの文面です
	リンクダウン	IntraGuardian本体の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信できないため、かなり遅延して発生します

	リンクアップ	IntraGuardian本体の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本体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ときは、ユーザーサポートへ問い合わせてください
	エンジン停止	IntraGuardian本体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本体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本体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本体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

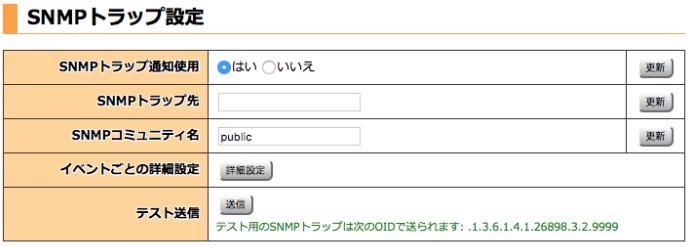
10-4-1. SYSLOG設定

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）スマート検知設定

本ソフトウェアが外部セキュリティ装置などと連動して登録済み端末の接続制御を行います。

10-5-1. SYSLOG検知設定

ルーターなどのネットワーク機器にSYSLOG転送の設定を行い、本ソフトウェアで対象となる登録済端末によるセキュリティアラートを検知して該当端末を直ちに排除状態にします。

SYSLOG検知使用	「**はい**」を選択すると以下の設定項目が表示され、設定内容が有効になります
待ち受けポート	SYSLOGをUDPで待ち受けるポート番号を整数で指定します
ログレベル	指定したSYSLOGログレベル以上のログが対象となります
ファシリティ	指定したSYSLOGファシリティのログが対象となります 全てを選択すると待ち受けているすべてのログが対象となります
エンコード	待ち受けているSYSLOGの文字コードを指定します
不正検知文字列	目的のログの文言に含まれる機器のIP(fromip)、対象の登録済み端末のMACアドレス(targetmac)とIPアドレス(targetip)を抽出して排除状態にできるように正規表現を使用した文字列を指定します 特定メーカのネットワーク機器がプリセットされています
許可検知文字列	もし、お持ちのネットワーク機器などからのSYSLOGにセキュリティアラートが解除されたことを通知する内容のSYSLOGが取得できる場合は、不正検知文字列と同様に正規表現を使用した文字列でfromip、targetmac、targetipを抽出できるようにします

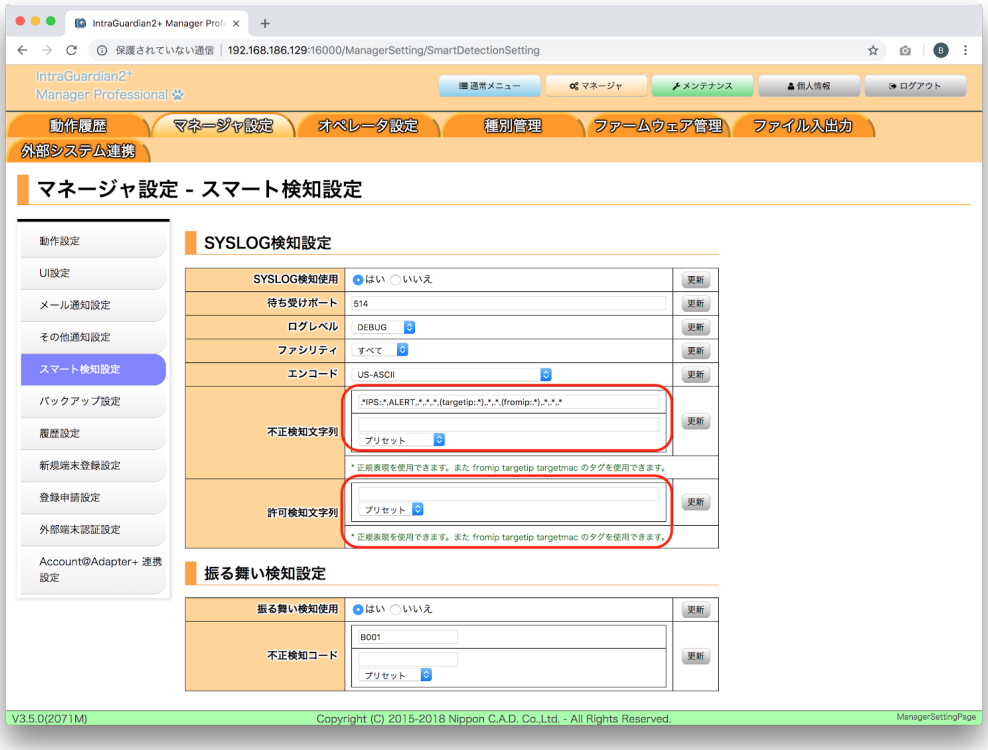
※ 不正検知文字列と許可検知文字列の正規表現には必ずtargetmacかtargetipのいずれかまたは両方の名前付きグループを記述してください

補足：スマート検知における正規表現の使用について

IntraGuardian2+ Manager Professional(以下マネージャ)のスマート検知機能を使用すると、IntraGuardian2+シリーズ以外のネットワーク機器やUTM装置(以下連携装置)からの不正検知の通知をトリガーとして不正端末を排除したり、または排除状態を解除することができます。（IntraGuardian2+シリーズのIntraGuardian SmartはUTMです）なお、IntraGuradian2+シリーズ製品に登録されていない端末は従来通り不正端末として扱われます。

SYSLOG検知の場合は、連携装置からの不正接続検知、又は不正接続状態の解除を受け取ったSYSLOGメッセージから認識します。連携装置からの指示は、正規表現にマッチするかで判断します。そのため、あらかじめどのようなメッセージを受け取るかを設定しておく必要があります。この不正検知文字列は正規表現で記述してください。詳しくは以下のサンプルを参考にしてください。

- マネージャのスマート検知設定画面



マネージャで以下のSYSLOGを検出したい場合は、上記画面赤枠のテキストフィールドに正規表現の例のように入力します。以下はサンプルのSYSLOGと正規表現の例です。

1806-3290002-M75S IPS: Aug 6 17:20:42,ALERT,2000361,Dropbox SSL Request,HTTPS,10.20.10.50,53118,LO,162.125.80.3,443,US,

上記IPSとALERTにそれぞれマッチ	10.20.10.50にマッチしてtargetipとして用いられる	162.125.80.3にマッチしてfromipとして用いられる
↓ ↓	↓	↓

.*IPS:.*,ALERT,.*,.*,.*,(targetip:.*),.*,.*,(fromip:.*),.*,.*,.*

スマート検知の設定で用いられる正規表現の表記法は、.NET Frameworkのライブラリで定義されているものを用います。正規表現についての詳しい情報は下記URLを参照してください。

https://msdn.microsoft.com/ja-jp/library/cc392020.aspx

補足：SYSLOG検知の優先順位

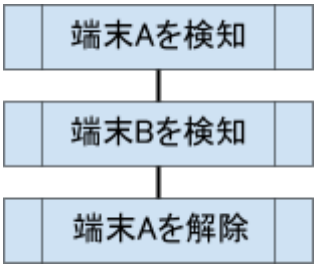
本機能は、fromipタグで指定されたネットワークのセクション内で、targetipタグで指定されたIPアドレスの登録端末、またはtargetmacタグで指定されたMACアドレスの登録端末を探し、それを一時的に不正端末として取り扱います。

もし、targetipかtargetmacが同時に指定されている場合、いずれかにマッチすれば動作します。
連続的に検知と解除が起きた場合は、その処理がシーケンシャルに動作し以下のような結果となります。

正規表現内で使用できるスマート検知用タグ一覧

fromip	外部のネットワーク機器のIPアドレス
targetip	検知対象の登録済みPCのIPアドレス
taregtmac	検知対象の登録済みPCのMACアドレス

- 動作例



上記の結果端末Aは許可状態になり、端末Bは検知状態になります。

10-5-2. 振る舞い検知設定(UTM連携)

※ 本設定は、IntraGuardian Smartと連携を行っているクラウド版マネージャのみ表示されます。

外部UTM機器からのログ出力のうち、指定された内部コードを持つセキュリティアラートを検知して、対象となる登録済み端末を排除状態にします。

振る舞い検知使用	「はい」を選択すると以下の設定項目が表示され、設定内容が有効になります
不正検知コード	外部UTM機器から送信されたセキュリティアラートに含まれる内部コードを指定します **※ IntraGuardian Smart用の不正通信検知の内部コードがプリセットされています**
許可検知コード	外部UTM機器から送信されたセキュリティアラート解除の通知に含まれる内部コードを指定します

※ IntraGuardian Smartは、許可検知コードに使用できる内部コードを持つセキュリティアラート解除の通知に対応していません。

10-6. （マネージャ設定）バックアップ設定

バックアップファイルを自動で作成することができます。
詳細は【17-5. 自動バックアップ設定】を参照してください。

※ クラウド版マネージャをご利用の場合は設定できません。

10-7. （マネージャ設定）履歴設定

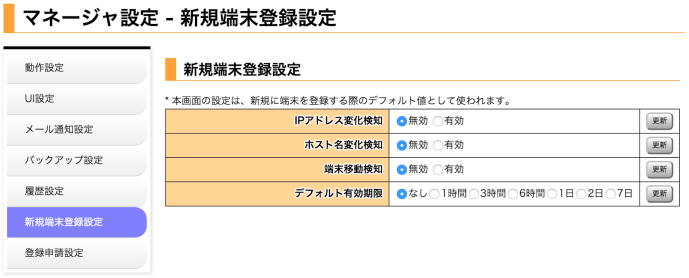
履歴設定では、動作履歴と端末履歴の取り扱いを設定することができます。
各項目の詳細は、【9-3. 新しい履歴と古い履歴】を参照してください。

※ 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設定します
端末履歴保存期間	端末履歴の保存期間を設定します
最近の履歴とする日数	「最近の履歴」とする日付を設定します
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 ※できる限りサーバ負荷の少ない時刻を指定することを推奨します
履歴整理	履歴整理を直ちに行います
履歴消去	履歴の全消去を直ちに行います

10-8. （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

10-9. （マネージャ設定）登録申請設定

登録申請機能に関する設定を行うことができます。
詳細は【14. 登録申請機能】を参照してください。

※ 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。

10-10. （マネージャ設定）外部端末認証設定

RADIUSサーバを利用して、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ための設定を行うことができます。

※ 外部端末認証により許可されていない端末でも、本ソフトウェアの端末登録で登録を行った端末の通信は許可されます。
※ 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アドレスが送信されます
外部認証応答待ち時間	認証サーバの認証応答待ち時間をミリ秒で指定します
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への切り替わり時間を分で指定します
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を秒で指定します
不正端末再認証時間	不正端末の再認証時間を秒で指定します

10-11. （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
許可するための設定を行うことができます。

※ 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+の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 ※ Account@Adapter+側の設定に合わせて指定してください
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+のサーバアドレスを指定します
外部認証サーバ(Slave)	Account@Adapter+のサーバアドレス（Slave）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値を指定します ※ 空欄の場合はMACアドレスが送信されます
外部認証応答待ち時間	認証サーバの認証応答待ち時間をミリ秒で指定します
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への切り戻し時間を分で指定します
登録セクション	認証成功時に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を秒で指定します
不正端末再認証時間	不正端末の再認証時間を秒で指定します

11. 管理者・オペレータの設定

11-1. 権限

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。
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。
オペレータは任意の人数を登録できます。

全権管理者以外のオペレータが本ソフトウェアを操作するためには、いずれかのセクションに管理権限、又は閲覧権限を持たせる必要があります。詳しくは【11-4. セクションの管理権限】を参照してください。

閲覧者	特定セクションの登録端末・不正接続一覧・設定状態を閲覧することができます
管理者	閲覧者の権限に加え、特定セクションの登録端末・不正端末の登録内容を変更することができます
システム管理者	管理者の権限に加え、特定セクションの設定・特定セクションの閲覧者・管理者・システム管理者の変更を行うことができます
全権管理者	全ての操作を行うことができます

11-2. オペレータ設定

オペレータ情報の閲覧・編集・削除を行うことができます。

※ 本画面は、全権管理者の権限を持ったオペレータのみ閲覧・操作することができます。

オペレータ設定は、現在登録されているオペレータの一覧が表示されます。
使用開始直後は、セットアップ時に登録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。

オペレータの情報として以下の項目を入力します。（名称に※が付いている項目は入力必須です）

< **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。既に登録してあ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※	ログイン時に使用する**パスワード**を指定します。
パスワード確認用※	確認のため、**パスワード**と同じ内容を入力します。
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。任意の文字列を入力できます**
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とき、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とき，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とき、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とき、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）とき、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とき、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とき、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端末が例外IPに登録されているIPアドレスで検知されたとき、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端末が例外ベンダに登録されているMACアドレスで検知されたとき、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とき、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とき、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有効期限が切れている登録端末をネットワーク内に検知したとき、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アドレスの利用を検知したとき、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のコンピュータ名が変化したとき、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のIPアドレスが変化したとき、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とき、通知するかどうかを指定します
端末登録	管理しているセクションで端末が新規登録されたとき、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本体がリンクアップしたとき、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本体の検知・排除システムが再起動したとき、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本体の検知・排除システムが停止したとき、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本体が本ソフトウェアと接続開始したとき、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本体が本ソフトウェアとの接続を切断したとき、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とき、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とき、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が新規登録されたとき、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が削除されたとき、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とき、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とき、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

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。設定項目は前述したオペレータの新規登録と同じです。

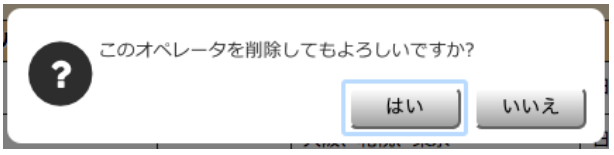
※ パスワードを変更しない場合は空欄にしてください。

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。

※ 操作中のオペレータ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

全権管理者以外のオペレータは自身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。

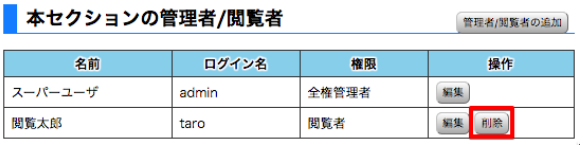
※ 個人情報画面はオペレータの変更と殆ど同じ内容ですが、変更を適用するためには現パスワードを入力する必要があります。
※ オペレータの新規作成や自分以外のオペレータ情報の変更は、全権管理者の権限を持ったオペレータしか操作することはできません。

11-4. セクションの管理権限

セクションの管理権限／閲覧権限を編集することができます。

11-4-1. セクションの管理権限／閲覧権限を付与する

オペレータにセクションの管理権限／閲覧権限を付与します。

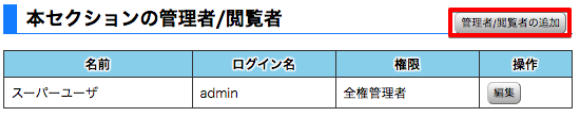


全権管理者以外のオペレータが本ソフトウェアを操作するためには、いずれかのセクションに管理権限、又は閲覧権限を持たせる必要があります。

※ 全権管理者は最初から全セクションに対して全ての操作が可能なため、本節の作業をする必要がありません。

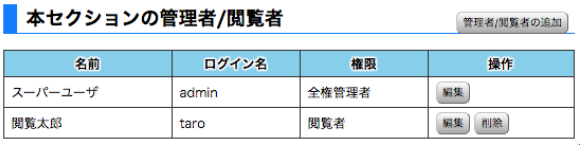
1. **通常メニュー**の**セクション管理**画面を表示します。そこで、**【3-3. 着目セクションの切り替え】**で説明した方法で、セクションを選択します。

2. 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。



3. 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、または閲覧することができるようになりました。

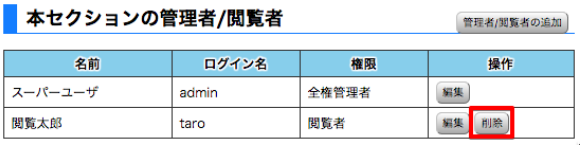


なお、セクションの管理権限は、下位の方向に継承します。つまり、「営業2課」に権限を持つオペレータは、自動的に「営業2課-東京」と「営業2課-札幌」にも権限を持つことになります。

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／閲覧権限を削除する

セクションに対するオペレータの管理権限／閲覧権限の剥奪は、通常メニューのセクション管理画面を用います。



割当を削除したいオペレータの「**削除**」ボタンをクリックすると、管理権限／閲覧権限を剥奪することができます。

※ ここで削除されるのは該当のセクションに対する管理権限／閲覧権限だけであり、オペレータ自身は削除されません。
※ 全権管理者は常に全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。
※ 上位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、権限を持っている最上位セクションを除いて権限欄に「(継承)」と付与表示され、「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。

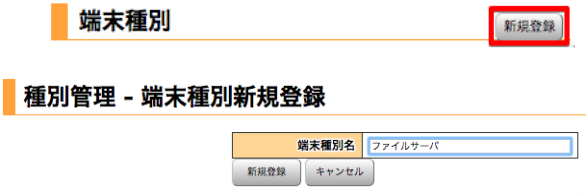
端末種別・NIC種別ともに、検知や排除の動作に影響はありません。端末を管理しやすくするための補助情報です。

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」等のOS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変更完了です。

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**」をクリックすると削除完了です。

※ 初期設定で「その他」と設定されている項目は削除できません。名称の変更は可能です。

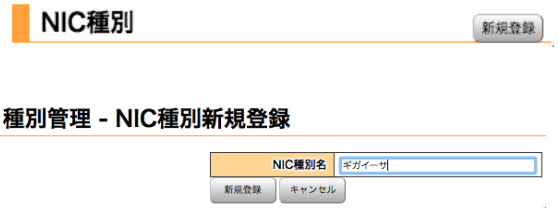
12-2. NIC種別

NIC種別は、ネットワークインタフェース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

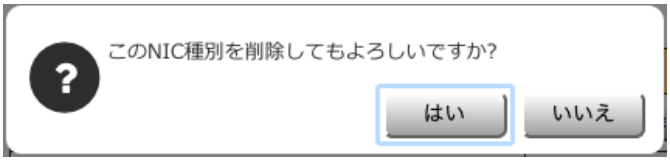
変更したいNIC種別の右側にある「**編集**」ボタンをクリックします。

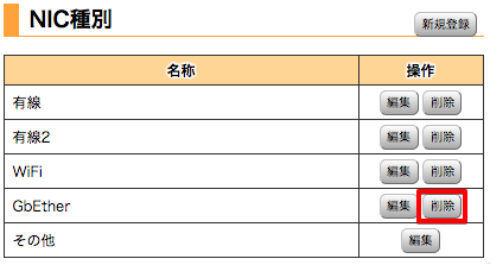
新しい「**NIC種別名**」を入力します。
入力が完了したら、「**変更**」ボタンをクリックし完了です。

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できません。名称の変更は可能です。

13. ファームウェア管理

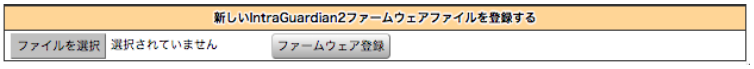
マネージャメニューの**ファームウェア管理**画面では、IntraGuardian本体に現在インストールされているファームウェアを確認し、バージョンアップを行うことが可能です。

上部には、本ソフトウェアに接続されている全てのIntraGuardian本体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が表示されます。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のファイル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、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する必要があります。

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ます。（ファームウェアファイルのダウンロードは、IntraGuardian本体の購入時にご登録いただいたIDとパスワードが必要です）



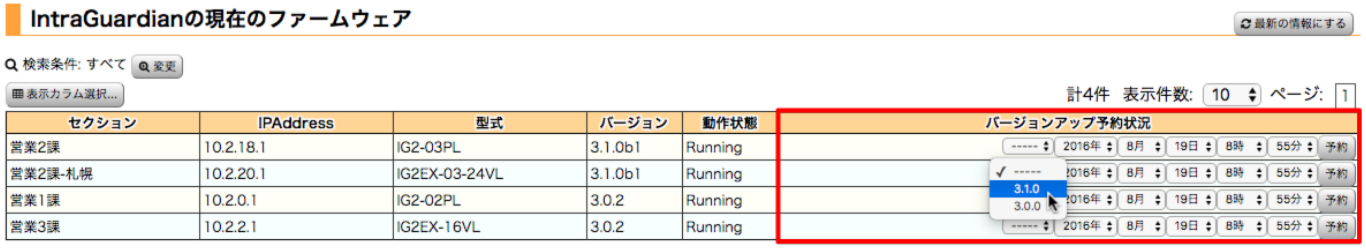
ファームウェア管理画面の下部にある「**ファイルを選択**」（ブラウザによっては「**参照...**」）と書かれた欄にダウンロードしたファームウェアファイルを指定し、「**ファームウェア登録**」ボタンをクリックします。

※ 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可能なIntraGuardian本体の型番を識別しますので、ダウンロードしたファームウェアファイルのファイル名は変更しないでください。

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ストレージ上にコピーされただけで、まだIntraGuardian本体へ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IntraGuardian本体の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のバージョンと、更新を実行する「**日時**」を選択し「**予約**」ボタンをクリックします。



指定した日時を経過すると、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認を行い、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）

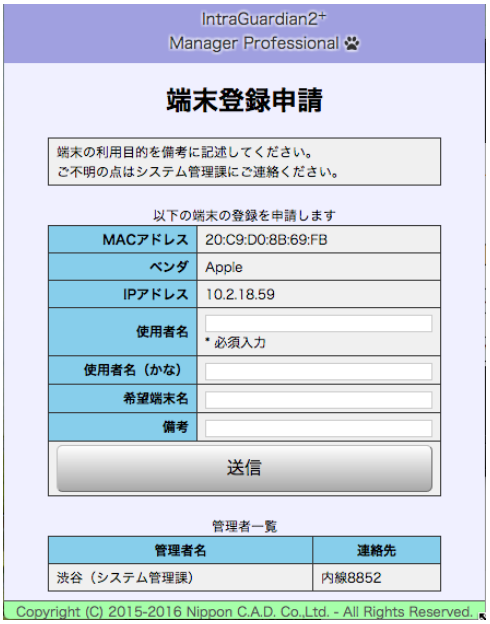
※ 本ソフトウェアに登録されているが、何らかの理由で通信できていないIntraGuardian本体に対してもバージョンアップを予約することができます。この場合、予約日時を経過してから通信を開始次第、バージョンアップ作業が行われます。

また、検索条件に合致する全てのIntraGuardian本体のフェームウェアを一括更新できます。

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、本ソフトウェアの管理者宛に申請要求を出すことができる機能です。



登録申請機能が有効化されているとき、排除されている端末でブラウザを使用して任意のサイトへ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フォームがブラウザに表示されます。

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

管理者が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、通常のネットワークアクセスが可能になります。

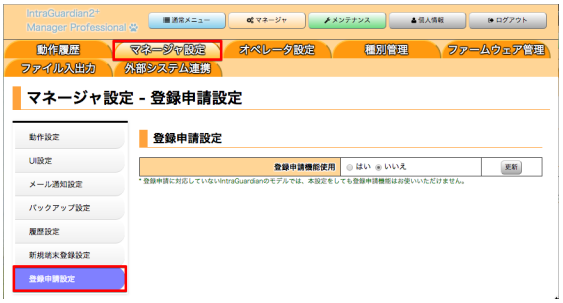
※ 本機能は、不正接続端末のOSやブラウザの種類や設定状態によっては有効に機能しない場合があります。
※ 本機能が有効なとき、登録済の端末から不正接続端末に対してHTTP接続をしようとすると申請画面が表示されます。
※ MACアドレスの全てのオクテットが「00」又は「FF」の場合、送信ボタンクリック後にエラーとなり申請は完了できません。

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、本ソフトウェアのマネージャ設定とIntraGuardian本体の両方を設定する必要があります。

14-2-1.（マネージャ設定）登録申請設定

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。

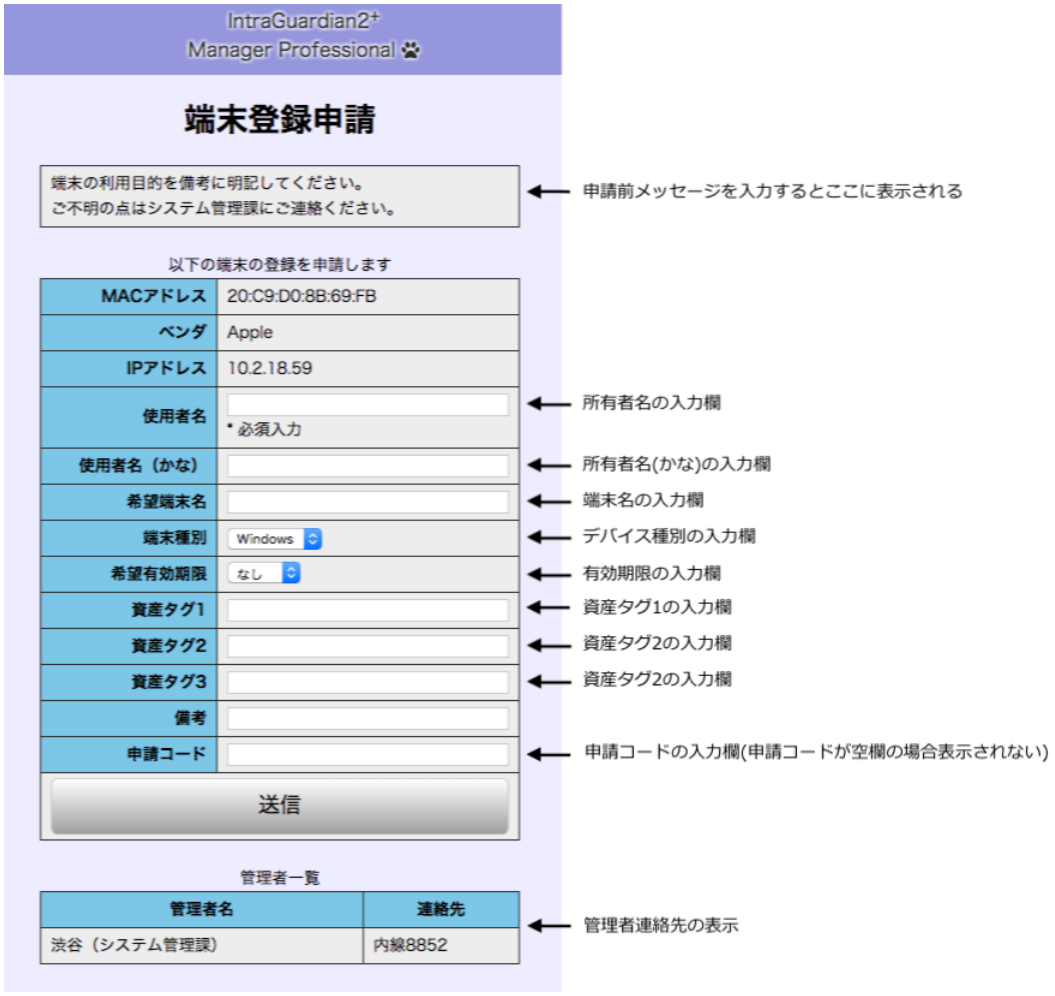


「**登録申請機能使用**」の「**はい**」を選択して「**更新**」をクリックすると、右図のように詳細な設定項目が入力できるようになりますので、各欄を入力して「**更新**」をクリックしてください。

< 登録申請設定項目 >

申請前メッセージ	記載したメッセージが不正接続端末のブラウザに表示されます
申請後メッセージ	記載したメッセージが申請送信後に表示されます
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**	登録申請画面に入力項目を追加します
管理者連絡先の表示	管理者への連絡先を不正接続端末に表示します
申請コード	申請コードを指定します ここで指定した申請コードと、申請者が不正接続端末の登録申請画面で入力した申請コードが一致しない場合、登録申請を受け付けません 本項目が空欄の場合、登録申請画面に申請コードの入力欄は表示されず、コード入力無しで申請できます
登録申請画面で用いる時間帯	「**有効期限の入力**」が有効化されていて、申請者が希望する有効期限を入力するときに使用する標準時を指定します
最大同時申請数	登録申請機能を一時的に無効化する申請数を指定します 異常な回数の登録申請が発生した場合のトラブル回避を想定しています
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します。PNGファイルを指定可能です

＜登録申請画面（不正端末に表示されます）＞



＜登録申請後画面（不正端末に表示されます）＞

14-2-2. 監視設定（IntraGuardian本体の設定）

IntraGuardian本体にも登録申請の有効化に必要な設定項目がありますので、本ソフトウェアからIntraGuardian本体の設定変更を行います。

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」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。

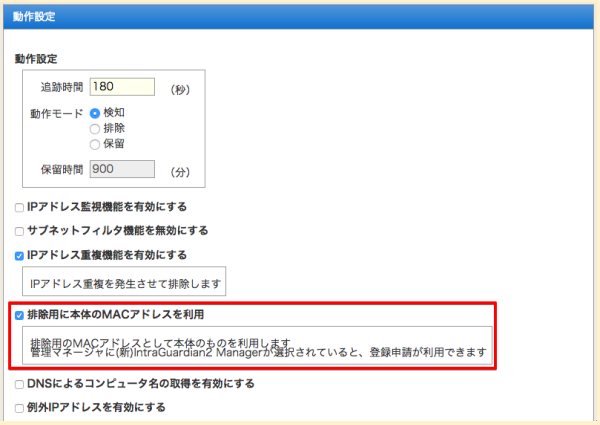
以上で、登録申請機能の有効化は完了です。

※ 本設定を行っても、IG2-03PL , IG2EX-03-08VL , IG2EX-03-24VL以外のIntraGuardian本体で登録申請機能は利用できません。

本設定を有効化して、マネージャ設定の登録申請機能を無効にしている場合、不正接続端末のブラウザへ左図が表示されます。

補足：IntraGuardian本体側の設定を確認

※ 本設定を有効にしたとき、該当のセクションで利用しているIntraGuardian本体のWebUI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。

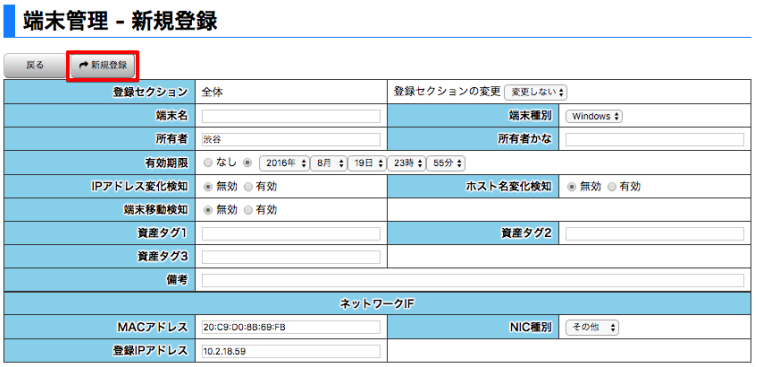


14-3. 登録申請一覧

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。
この画面で、着目しているセクション、及びその下位セクションで申請中の端末を一覧できます。

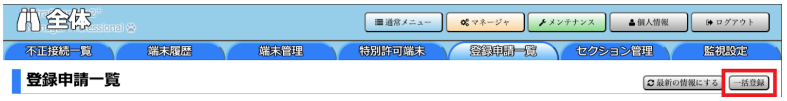
表の1行をクリックするか、右端の「**登録**」ボタンをクリックすると、端末の新規登録画面が表示されます。

登録申請者が指定した情報があると、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分程度で登録情報がIntraGuardian本体へ送信されます。
すると、IntraGuardian本体はこの端末に対する排除処理を停止し、この端末は通常のネットワークアクセスが可能になります。

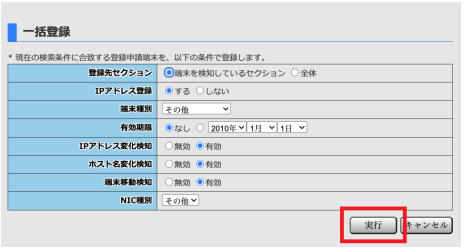


※ 当該端末やルータなどのネットワーク機器が記憶した偽のARP情報を完全に忘れるまでの間（一般的には数分程度）は、ネットワークへのアクセスが不安定になることがあります。
※ MACアドレスの全てのオクテットが「00」又は「FF」の場合、新規登録ボタンをクリック後にエラーとなり、申請を完了できません。

登録申請一覧に表示されている端末を一括で登録する場合は、「**一括登録**」ボタンをクリックしてください。

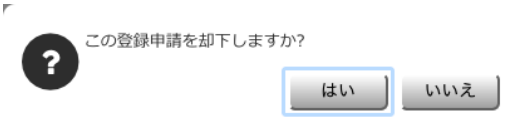


一括登録ボタンをクリックすると登録の条件を設定するポップアップが表示されますので、条件を確認後「**実行**」ボタンをクリックすると一括登録されます。



申請が不正なものであるなどの理由で許可しない場合は、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画面が表示されますので、拒否する場合は「**はい**」ボタン、拒否しない場合は「**いいえ**」ボタンをクリックしてください。



申請情報は、登録又は拒否を行うまで登録申請一覧に残り続けます。

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で、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。

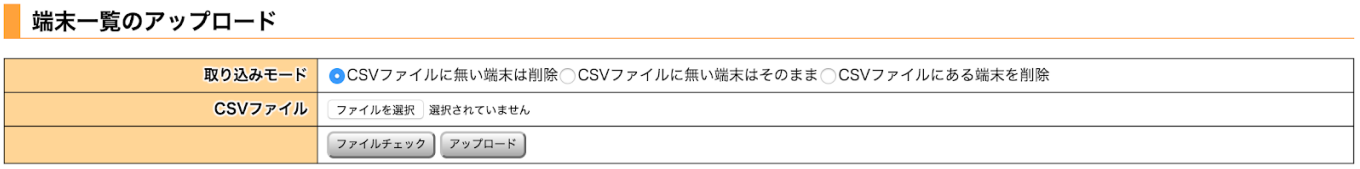
15-1. 端末一覧のダウンロード

端末一覧のダウンロードを行うことができます。
「**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ファイルとして出力することが可能です。
CSVファイルのフォーマットは、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

端末一覧のアップロード、又はファイルチェックを行うことができます。
取り込みモードとCSVファイルを選択して実行します。

※ 「端末一覧のアップロード」は、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。



取り込みモード： CSVファイルに無い端末は削除	登録端末一覧を全て入れ直すことができます
取り込みモード： CSVファイルに無い端末はそのまま	CSVファイルに記述されている端末を追加することができます
取り込みモード： CSVファイルにある端末を削除	CSVファイル中の端末名以外の記述は全て無視され、記述された端末の登録が削除されます
CSVファイル	「**ファイルを選択**」（ブラウザによっては「**参照...**」）でCSVファイルを指定します
ファイルチェック	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
アップロード	取り込みモードに従って、CSVファイルの情報を本ソフトウェアのデータベースへ取り込みます **※ MACアドレスの全てのオクテットが「00」又は「FF」の行は取り込み行数に含まれますが、実際には対象から除外されます**

補足：端末一覧のCSVファイルの仕様

「**端末一覧のアップロード**」で取り込むCSVファイルは、次の基本フォーマットに従う必要があります。

- 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を指定可能ですが、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のご利用を強く推奨します。
  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、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する必要があります。

15-3. 端末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。

15-3-1.端末CSVファイルフォーマットで出力する項目

端末CSVファイルフォーマットの上部は、出力する項目の選択とその並び順の指定です。

出力	順番変更	カラム名	内容
☑	⇈ ↑ ↓ ⇊	Section	登録セクション
☑	⇈ ↑ ↓ ⇊	Name	端末名
☑	⇈ ↑ ↓ ⇊	DeviceType	端末種別
☑	⇈ ↑ ↓ ⇊	OwnerName	所有者
☑	⇈ ↑ ↓ ⇊	OwnerRuby	所有者かな
☑	⇈ ↑ ↓ ⇊	ExpireTime	有効期限
☑	⇈ ↑ ↓ ⇊	IgnoreIPChange	IPアドレス変化検知
☑	⇈ ↑ ↓ ⇊	IgnoreHostnameChange	ホスト名変化検知
☑	⇈ ↑ ↓ ⇊	IgnoreDeviceCarry	端末移動検知
☑	⇈ ↑ ↓ ⇊	AssetTag1	資産タグ1
☑	⇈ ↑ ↓ ⇊	AssetTag2	資産タグ2
☑	⇈ ↑ ↓ ⇊	AssetTag3	資産タグ3
☑	⇈ ↑ ↓ ⇊	Hostname	ホスト名
☑	⇈ ↑ ↓ ⇊	Workgroup	ワークグループ
☑	⇈ ↑ ↓ ⇊	HostOS	OS名
☑	⇈ ↑ ↓ ⇊	HostType	OS種別
☑	⇈ ↑ ↓ ⇊	Note	備考
☑	⇈ ↑ ↓ ⇊	Created	登録日時
☑	⇈ ↑ ↓ ⇊	Modified	最終更新日時
☑	⇈ ↑ ↓ ⇊	Lladdr	MACアドレス
☑	⇈ ↑ ↓ ⇊	LladdrType	NIC種別
☑	⇈ ↑ ↓ ⇊	Registeredlpaddr	登録IPアドレス
☑	⇈ ↑ ↓ ⇊	Ipaddr	現在IPアドレス
☑	⇈ ↑ ↓ ⇊	DetectTime	初検知日時
☑	⇈ ↑ ↓ ⇊	ConfirmedTime	確認日時
☑	⇈ ↑ ↓ ⇊	Op	MACアドレス追加オプション

「**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、後ろの行のデータが優先され、前の行は上書きされます。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拠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「+」以外を記述しないでください。

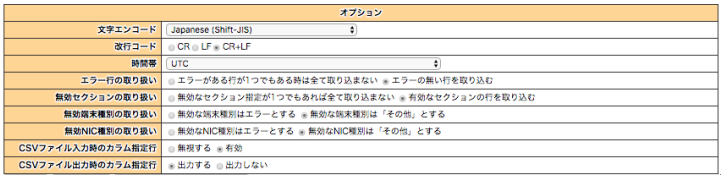
CSVファイルの1行目が「#」で始まっていない場合、又はCSVフォーマットオプションの「**CSVファイル入力時のカラム指定行**」に「**無視する**」が指定されている場合、各行はCSVフォーマットオプションで指定されたカラム順にデータが並んでいるものとして処理されます。

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。

15-3-2.端末CSVファイルフォーマットのオプション設定

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。



文字エンコード	入出力に用いる文字コードを指定します
改行コード	出力に用いる改行コードを指定します 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標準帯を指定します
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を指定します 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を指定します 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を指定します 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を指定します 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を指定します
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を指定します

※ 「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（セクション名カラムが無いか、又はセクション名が空欄である）場合、「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

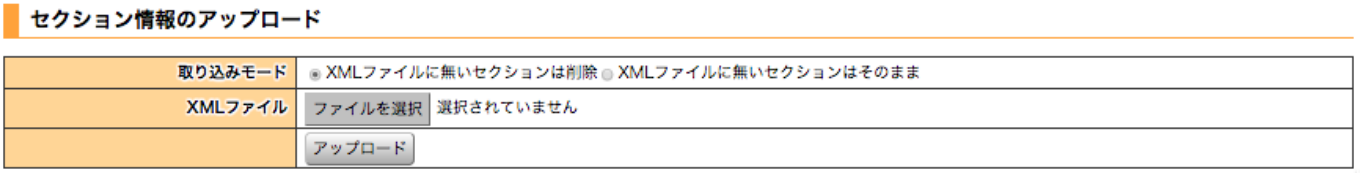
セクション情報のダウンロードを行うことができます。

「**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ファイルとして出力できます。
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。

15-5. セクション情報のアップロード

セクション情報のアップロードを行うことができます。
取り込みモードとXMLファイルを選択して実行します。

※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。



取り込みモード：XMLファイルに無いセクションは削除	全セクションを入れ直すことができます
取り込みモード：XMLファイルに無いセクションはそのまま	XMLファイルに記述されているセクションを追加することができます
XMLファイル	「**ファイルを選択**」（ブラウザによっては「**参照...**」）でXMLファイルを指定します
アップロード	取り込みモードに従って、XMLファイルに記述されている情報を本ソフトウェアのデータベースへ取り込みます

補足：セクション情報のXMLファイルの仕様

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ノードは全て無視されます。（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**
ルート要素です。

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**
セクションの定義です。

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**
親セクション指定です。
当該セクション名は既に定義されている必要があります。
ルートセクション以外では必ず1つ以上存在する必要があります。

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**
オペレータの定義です。
section要素内に記述されている場合、そのセクションの管理／閲覧者であることを示しています。

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です。
本要素が存在する場合、該当のオペレータへ通知が行なわれます。

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**
ネットワークの定義です。

上位タグ	section
下位タグ	なし

属性名		説明
address	必須	（IntraGuardian本体の）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ません。

タグ名: **ig**
IntraGuardian本体の定義です。

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本体の設定カテゴリです。
該当のカテゴリ内の設定が全てデフォルト値の場合、category要素は出力されません。

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本体の設定です。
該当する項目の設定がデフォルト値の場合、config要素は出力されません。

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アドレスです。

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属性のいずれかが必要です。
start属性がある場合、end属性は必須です。

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

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

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用すると、**【15. ファイル入出力】**と同様の操作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連携するときに利用してください。

※ 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。

16-1. 端末一覧書き出し

端末一覧のCSVファイルを、ローカルディレクトリ、又はFTPサーバへ書き出すことができます。

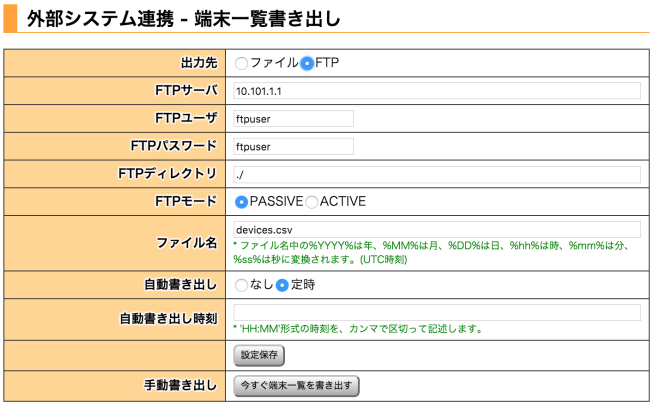
16-1-1. 指定ディレクトリへの保存

端末一覧CSVファイルを、特定のディレクトリへ書き出すことができます。
時刻を指定した自動書き出しも可能です。

出力先	「**ファイル**」を選択します
ディレクトリ	出力先のローカルディレクトリを指定します ※ ネットワークサーバへ保存する場合、「16-1-2. FTPへの保存」を参照してください
ファイル名	ファイル名を指定します。ファイル名は変数を指定可能です 年：%YYYY% 月：%MM% 日：%DD% 時：%HH% 分：%MM% 秒：%SS% ※ 全てUTC時刻になります
自動書き出し	「**定時**」を選択すると、「**自動書き出し時刻**」に従って毎日CSVファイルを出力します
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
設定保存	クリックすると設定が保存されます
手動書き出し	「**今すぐ端末一覧を書き出す**」ボタンをクリックすると、クリック時点の情報を書き出すことができます

16-1-2. FTPへの保存

端末一覧CSVファイルを、FTPサーバへアップロードさせることができます。
時刻を指定した自動アップロードも可能です。



出力先	「**FTP**」を選択します
FTPサーバ	FTPサーバをIPアドレス、又はホスト名で指定します **※ ホスト名で指定する場合、本ソフトウェアをセットアップしたサーバの名前解決を確認の上で利用してください**
FTPユーザ	FTPサーバのユーザ名を指定します
FTPパスワード	FTPサーバのパスワードを指定します
FTPディレクトリ	ファイルをアップロードするディレクトリを指定します
FTPモード	パッシブ／アクティブを指定します
ファイル名	ファイル名を指定します。ファイル名は変数を指定可能です 年：%YYYY% 月：%MM% 日：%DD% 時：%HH% 分：%MM% 秒：%SS% **※ 全てUTC時刻になります**
自動書き出し	「**定時**」を選択すると、「**自動書き出し時刻**」に従って毎日CSVファイルを出力します
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
設定保存	クリックすると設定が保存されます
手動書き出し	「**今すぐ端末一覧を書き出す**」ボタンをクリックすると、クリック時点の情報を書き出すことができます

16-2. 端末一覧取り込み

端末一覧のCSVファイルを、ローカルディレクトリ、又はFTPサーバから取り込むことができます。

16-2-1. 指定ディレクトリからの取り込み

端末一覧CSVファイルを、特定のディレクトリ内から取り込むことができます。
時刻を指定した自動取り込みも可能です。

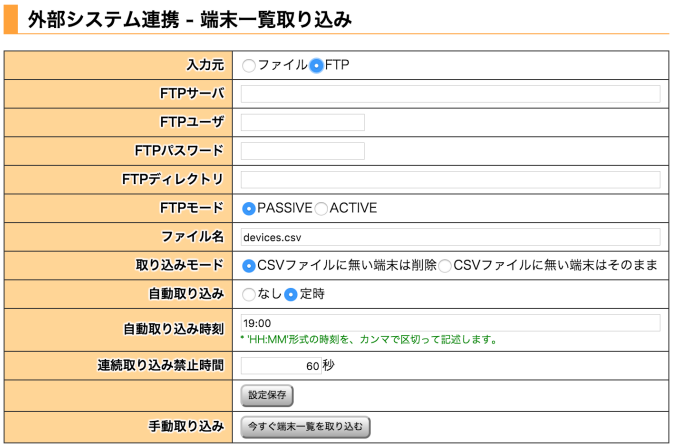
※ MACアドレスの全てのオクテットが00またはFFの行は取り込み行数に含まれますが、実際は対象から除外されます。

入力先	「**ファイル**」を選択します
ディレクトリ	端末一覧CSVが保存されているローカルディレクトリを指定します。 **※ ネットワークサーバから取り込む場合、「16-2-2. FTPからの取り込み」を参照してください**
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ときは「**CSVファイルに無い端末は削除**」、CSVの内容を追加登録として取り扱うときは「**CSVファイルに無い端末はそのまま**」を選択します
自動取り込み	「**定時**」を選択すると、「**自動書き出し時刻**」に従って毎日CSVファイルを取り込みます
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
設定保存	クリックすると設定が保存されます
手動取り込み	「**今すぐ端末一覧を取り込む**」ボタンをクリックすると、クリック時点の情報を書き出すことができます

16-2-2. FTPからの取り込み

端末一覧CSVファイルを、FTPサーバから取り込むことができます。
時刻を指定した自動取り込みも可能です。

※ MACアドレスの全てのオクテットが00またはFFの行は取り込み行数に含まれますが、実際は対象から除外されます。



入力先	「**FTP**」を選択します
FTPサーバ	FTPサーバをIPアドレス、又はホスト名で指定します **※ ホスト名で指定する場合、本ソフトウェアをセットアップしたサーバの名前解決を確認の上で利用してください**
FTPユーザ	FTPサーバのユーザ名を指定します
FTPパスワード	FTPサーバのパスワードを指定します
FTPディレクトリ	FTPサーバ上のディレクトリを指定します
FTPモード	パッシブ／アクティブを指定します
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ときは「**CSVファイルに無い端末は削除**」、CSVの内容を追加登録として取り扱うときは「**CSVファイルに無い端末はそのまま**」を選択します
自動取り込み	「**定時**」を選択すると、「**自動書き出し時刻**」に従って毎日CSVファイルを取り込みます
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
設定保存	クリックすると設定が保存されます
手動取り込み	「**今すぐ端末一覧を取り込む**」ボタンをクリックすると、クリック時点の情報を書き出すことができます

16-3. 端末CSVフォーマット

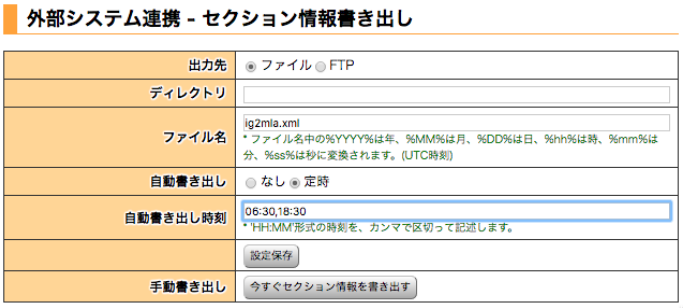
端末一覧の入出力に用いるCSVのフォーマットオプションを指定できます。
設定内容は【15-3. CSVファイルフォーマット】と同様のため、そちらを参照してください。

16-4. セクション情報書き出し

セクション情報のXMLファイルを、ローカルディレクトリ、又はFTPサーバへ書き出すことができます。

16-4-1. 指定ディレクトリへの保存

セクション情報のXMLファイルを、特定のディレクトリへ書き出すことができます。
時刻を指定した自動書き出しも可能です。



出力先	「**ファイル**」を選択します
ディレクトリ	出力先のローカルディレクトリを指定します **※ ネットワークサーバへ保存する場合、「16-4-2. FTPへの保存」を参照してください**
ファイル名	ファイル名を指定します。ファイル名は変数を指定可能です 年：%YYYY% 月：%MM% 日：%DD% 時：%HH% 分：%MM% 秒：%SS% **※ 全てUTC時刻になります**
自動書き出し	「**定時**」を選択すると、「**自動書き出し時刻**」に従って毎日XMLファイルを出力します
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
設定保存	クリックすると設定が保存されます
手動書き出し	「**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、クリック時点の情報を書き出すことができます

16-4-2. FTPへの保存

セクション情報のXMLファイルを、FTPサーバへアップロードすることができます。
時刻を指定した自動書き出しも可能です。

出力先	「**FTP**」を選択します
FTPサーバ	FTPサーバをIPアドレス、又はホスト名で指定します **※ ホスト名で指定する場合、本ソフトウェアをセットアップしたサーバの名前解決を確認の上で利用してください**
FTPユーザ	FTPサーバのユーザ名を指定します
FTPパスワード	FTPサーバのパスワードを指定します
FTPディレクトリ	ファイルをアップロードするディレクトリを指定します
FTPモード	パッシブ／アクティブを指定します
自動書き出し	「**定時**」を選択すると、「**自動書き出し時刻**」に従って毎日XMLファイルを出力します
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
設定保存	クリックすると設定が保存されます
手動書き出し	「**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、クリック時点の情報を書き出すことができます

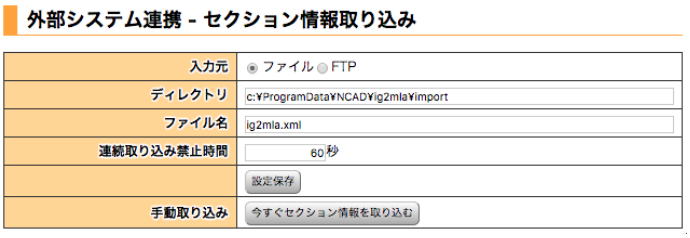
16-5. セクション情報取り込み

セクション情報のXMLファイルを、ローカルディレクトリ、又はFTPサーバから取り込むことができます。

※ 現状、セクション情報の取り込みを定時に実行することはできません。

16-5-1. 指定ディレクトリからの取り込み

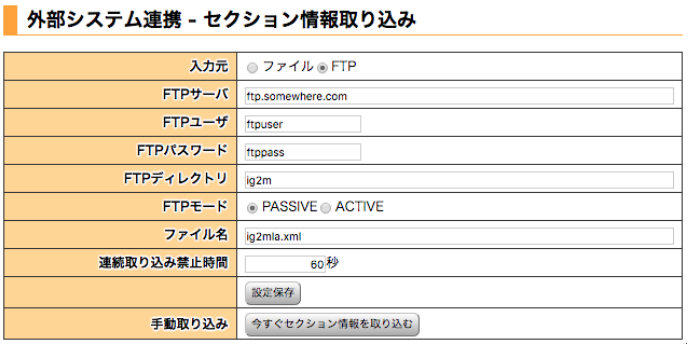
セクション情報のXMLファイルを、指定のディレクトリから取り込むことができます。



入力先	「**ファイル**」を選択します
ディレクトリ	セクション情報のXMLファイルが保存されているローカルディレクトリを指定します **※ ネットワークサーバから取り込む場合、「16-5-2. FTPからの取り込み」を参照してください**
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、セクション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
設定保存	クリックすると設定が保存されます
手動取り込み	「**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、クリック時点の情報を取り込むことができます

16-5-2. FTPからの取り込み

セクション情報のXMLファイルを、FTPサーバから取り込むことができます。



入力先	「FTP」を選択します
FTPサーバ	FTPサーバをIPアドレス、又はホスト名で指定します **※ホスト名で指定する場合、本ソフトウェアをセットアップしたサーバの名前解決を確認の上で利用してください**
FTPユーザ	FTPサーバのユーザ名を指定します
FTPパスワード	FTPサーバのパスワードを指定します
FTPディレクトリ	FTPサーバ上のディレクトリを指定します
FTPモード	パッシブ／アクティブを指定します
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、セクション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
設定保存	クリックすると設定が保存されます
手動取り込み	「**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、クリック時点の情報を取り込むことができます

17. バックアップ・復元

本ソフトウェアが使用するデータベースをバックアップ、及び復元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利用できません。

17-1. バックアップのダウンロード

データベースを一つのファイルにバックアップし、ブラウザでダウンロードすることができます。

バックアップ先	「**ダウンロード**」を選択します
バックアップ内容	全部　　：全て（※1）のデータをバックアップ対象とします 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します 履歴をすべて除く：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します **※1 履歴データを含むとファイルサイズが大きくなります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**
バックアップファイル暗号化キー	バックアップファイルの復元時に暗号化キーを利用する場合、入力します
ダウンロード	クリックすると、バックアップファイルをダウンロードします

17-2. バックアップのファイル保存

データベースを一つのファイルにバックアップし、指定のディレクトリへ保存することができます。
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。

バックアップ先	「**ファイル保存**」を選択します
バックアップ内容	全部　　：全て（※1）のデータをバックアップ対象とします 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します 履歴をすべて除く：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します **※1 履歴データを含むとファイルサイズが大きくなります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**
バックアップファイル暗号化キー	バックアップファイルの復元時に暗号化キーを利用する場合、入力します
ディレクトリ	保存先のディレクトリをフルパス(絶対パス)で入力します
ファイル作成	クリックすると、バックアップファイルを保存します

17-3. バックアップのFTP保存

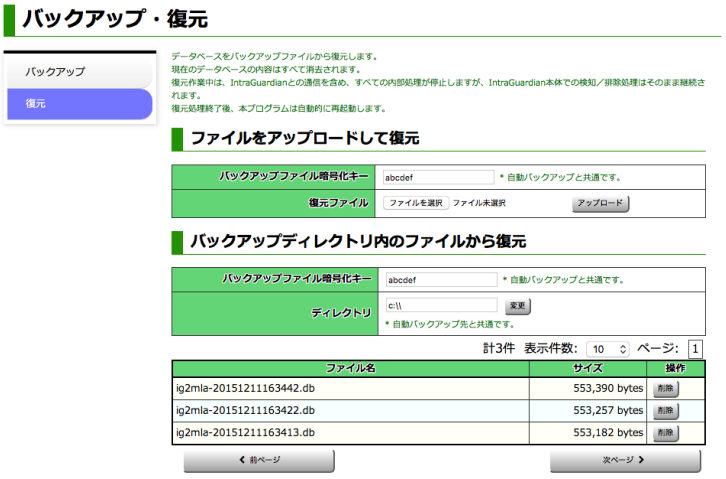
データベースを一つのファイルにバックアップし、指定のFTPサーバへアップロードすることができます。
作成されるファイルは「**バックアップのダウンロード**」と同様のファイルです。

バックアップ先	「**FTP保存**」を選択します
バックアップ内容	全部　　：全て（※1）のデータをバックアップ対象とします 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します 履歴をすべて除く：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します **※1 履歴データを含むとファイルサイズが大きくなります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**
バックアップファイル暗号化キー	バックアップファイルの復元時に暗号化キーを利用する場合、入力します
FTPサーバ	FTPサーバをIPアドレス、又はホスト名で指定します **※ ホスト名で指定する場合、本ソフトウェアをセットアップしたサーバの名前解決を確認の上で利用してください**
FTPユーザ	FTPサーバのユーザ名を指定します
FTPパスワード	FTPサーバのパスワードを指定します
FTPディレクトリ	FTPサーバ上のディレクトリを指定します
FTPモード	パッシブ／アクティブを指定します
実行	クリックするとバックアップファイルをアップロードします

17-4. 復元

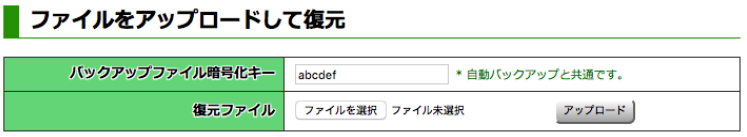
自動バックアップ、又は手動バックアップにて作成されたバックアップファイルから設定を復元することができます。

※ 復元をおこなうと、現在のデータベースの内容は全消去されます。
※ 復元作業中はIntraGuardian本体との通信を含めて全ての内部処理が停止しますが、IntraGuardian本体による検知／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を直接選択して復元を行います。



バックアップファイル暗号化キー	バックアップファイルの作成時に設定した暗号化キーを入力します 暗号化されていない場合は空欄にします
復元ファイル	「**ファイルを選択**」をクリックし、バックアップファイルを選択します
アップロード	クリックすると「**復元ファイル**」で指定したバックアップファイルから復元します **※ バックアップファイルのサイズが大きい場合、復元に時間がかかる場合があります**

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

本ソフトウェアと同一のサーバー内のディレクトリにバックアップしたバックアップファイルから復元を行います。

バックアップファイル暗号化キー	バックアップファイルの作成時に設定した暗号化キーを入力します 暗号化されていない場合は空欄にします
ディレクトリ	バックアップファイルが保存されているディレクトリを指定します **※ ディレクトリを変更する場合、ディレクトリのパスを入力し「変更」ボタンをクリックします**
ファイル名	「**ディレクトリ**」で指定したディレクトリに置かれているバックアップファイルの一覧が表示されます バックアップファイルのファイル名をダブルクリックすると、クリックしたバックアップファイルから復元します **※バックアップファイルのサイズが大きい場合、復元に時間がかかる場合があります**

17-5. 自動バックアップ設定

バックアップファイルを自動で作成することができます。

※ 本設定は、「マネージャ」メニューの「マネージャ設定」画面の「バックアップ設定」で行います。
※ いくつかの設定内容は、「メンテナンス」メニューの「バックアップ・復元」画面の「バックアップ」と共通となっており、異なる設定を入力することはできません。
（「バックアップ・復元」画面の「バックアップ」の該当項目の設定欄に「* 自動バックアップと共通です。」又は「* 自動バックアップ先と共通です。」と記載されています）
※ クラウド版マネージャをご利用の場合は設定できません。

17-5-1. ファイル保存方式の自動バックアップ

ファイル保存方式で自動バックアップを設定します。
設定変更の反映は、各項目右の「**更新**」ボタンを都度クリックしてください。

バックアップファイル暗号化キー	バックアップファイルの復元時に暗号化キーを利用する場合、入力します
自動バックアップ	「**はい**」を選択すると自動バックアップを有効化します
自動バックアップ時刻	自動バックアップの時刻を指定します
自動バックアップ内容	全部　：全て（※1）のデータをバックアップ対象とします 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します 履歴をすべて除く：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します ※1 履歴データを含むとファイルサイズが大きくなります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
バックアップ先	「**ファイル保存**」を選択します
バックアップ先ディレクトリ	保存先のディレクトリをフルパス(絶対パス)で入力します
バックアップ先ディレクトリ容量	バックアップ先のストレージを圧迫しないよう、専有する容量の上限を指定することができます

17-5-2. FTP保存方式の自動バックアップ

FTP保存方式で自動バックアップを設定します。設定変更の反映は、各項目右の「**更新**」ボタンを都度クリックしてください。

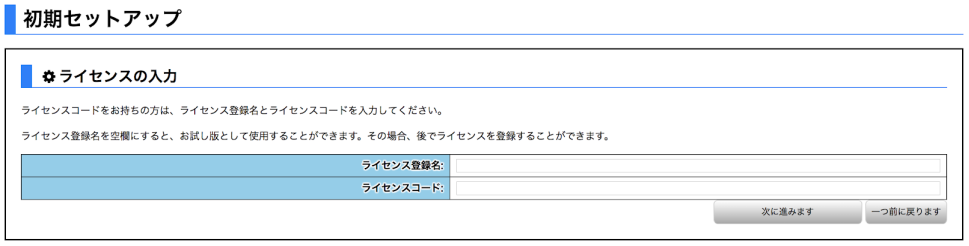
バックアップファイル暗号化キー	バックアップファイルの復元時に暗号化キーを利用する場合、入力します
自動バックアップ	「**はい**」を選択すると自動バックアップを有効化します
自動バックアップ時刻	自動バックアップの時刻を指定します
自動バックアップ内容	全部　　：全て（※1）のデータをバックアップ対象とします 古い履歴を除く　：最近の履歴とする日数（※2）を超える履歴を除く全てのデータをバックアップ対象とします 履歴をすべて除く：履歴データ（動作履歴、端末履歴）を除くデータをバックアップ対象とします **※1 履歴データを含むとファイルサイズが大きくなりますのでご注意ください** **※2 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**
バックアップ先	「**FTP保存**」を選択します
FTPサーバ	FTPサーバをIPアドレス、又はホスト名で指定します **※ ホスト名で指定する場合、本ソフトウェアをセットアップしたサーバの名前解決を確認の上で利用してください**
FTP接続ユーザ名	FTPサーバのユーザ名を指定します
FTP接続パスワード	FTPサーバのパスワードを指定します
FTPディレクトリ	FTPサーバ上のディレクトリを指定します
FTPモード	パッシブ／アクティブを指定します

18. ライセンスコードの登録

製品版、又は無償版のライセンスコードを登録します。

18-1. 初期セットアップ時のライセンスの入力

初期セットアップ時のウィザードで「**ライセンスの入力**」が表示されます。
本ソフトウェアの購入時に発行された「**ライセンス登録名**」と「**ライセンスコード**」を入力します。

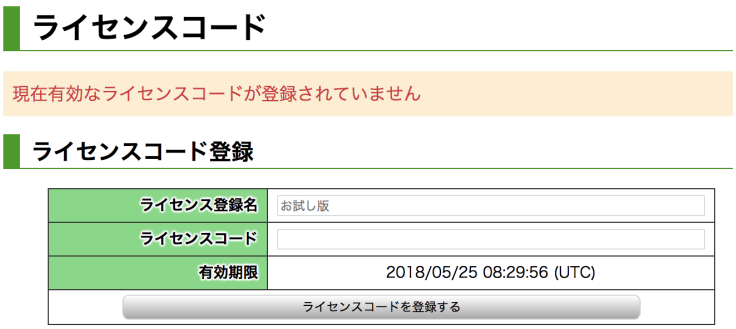


※ 無償版のライセンスコードを入力した場合、作成可能なセクション数が9個に制限されます。

18-2. 評価版として利用する

初期セットアップ時、ライセンス情報を入力せずにセットアップ作業を完了することができます。その場合、本ソフトウェアを評価版として利用することができます。

※ 評価版の使用期限は30日間です。



18-3. セットアップ後にライセンスコードを入力する

セットアップしてからライセンスコードを入力することができます。
「**メンテナンス**」メニューの「**ライセンスコード**」画面から、本ソフトウェアのライセンスコードをいつでも登録することが可能です。

正規の「**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。

※ 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。
※ ライセンス登録名、及びライセンスコードは、空白、及び全角／半角を区別しますので入力を確実に行ってください。

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**」画面から、本ソフトウェアをアップグレードすることができます。

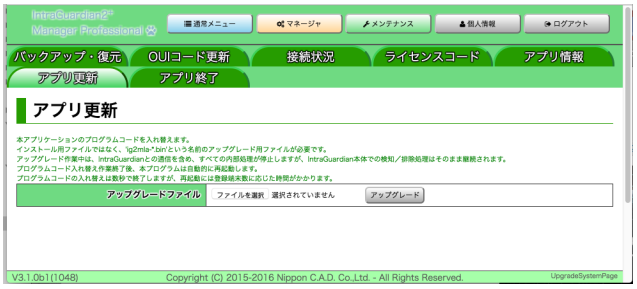
※ 本画面は、クラウド版マネージャをご利用の場合は操作できません。

19-1. アップグレードファイルの入手

アップグレードファイルは、公式サイト (https://intraguardian.jp) のファームウェアダウンロードから入手できます。

※ ダウンロードは、購入後のライセンス登録時に発行される「ログインID」と「パスワード」が必要です。
※ アップグレードファイルは拡張子が「bin」になっており、初回セットアップ時のインストーラー（拡張子が「exe」）とファイル形式が異なります。
※ 無償版を利用などの理由でアップグレードファイルを入手できない場合、旧バージョンのアンインストールを行った後、新バージョンのインストーラーを利用してください。

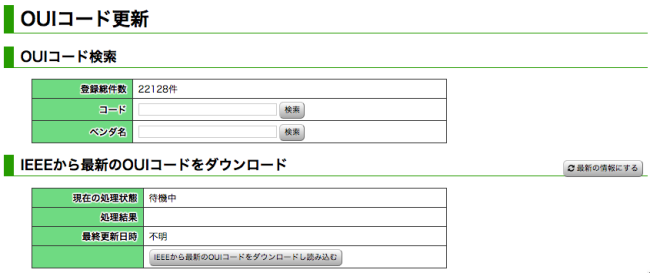
19-2. アップグレード



本ソフトウェアへ全権管理者でログインし、「**メンテナンス**」メニューの「**アプリ更新**」画面を表示します。
「**ファイルを選択**」をクリックして、入手したアップグレードファイルを選択し、「**アップグレード**」ボタンをクリックしてください。本ソフトウェアがアップグレードされ、自動的に再起動します。
ここで必ず、本ソフトウェアをインストールしたWindowsを再起動を行ってから本ソフトウェアへ再度ログインし、動作確認を行ってください。

20. OUIコード更新

OUIコードの更新や検索を行うことができます。



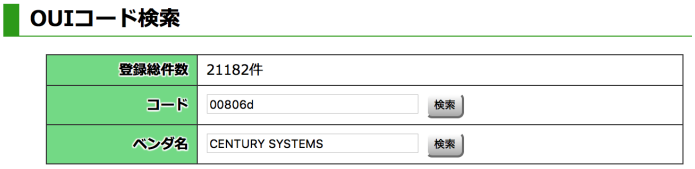
OUIコードとは

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のメーカー毎に割り当てられています。メーカー毎のOUIコードは技術標準化機関のIEEEが管理しており、OUIコードのデータベースがインターネットに公開されています。本ソフトウェアはOUIコードのデータベースを利用し、「通常メニュー」の各タブのMACアドレス欄に**ベンダの名称を表示**することができます。

20-1. OUIコード検索

「**コード**」(MACアドレス)、又は「**ベンダ名**」を入力して検索し、相互に表示することができます。

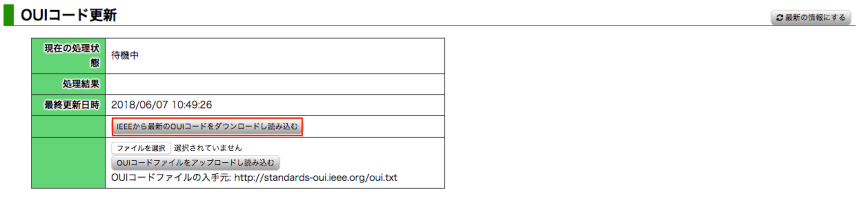
※予め、OUIコードのデータベースを本ソフトウェアへ適用しておく必要があります。



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

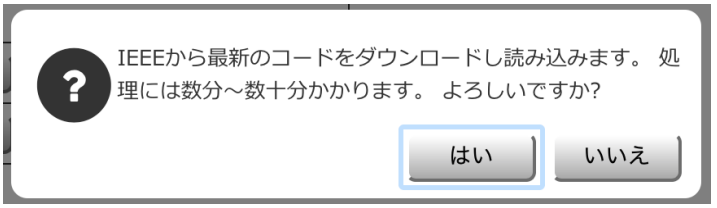
20-2. IEEEから最新のOUIコードをダウンロード

IEEEからOUIコードをダウンロードし、本ソフトウェアのデータベースへ適用することができます。



「**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。

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。



20-3. OUIコードファイルをアップロード

入手済のOUIコードのデータベースファイルを、本ソフトウェアへアップロードして適用することができます。

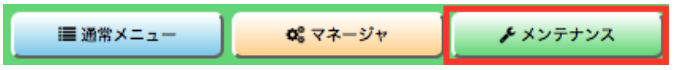
「**ファイルを選択**」ボタンをクリックしてOUIコードのファイルを指定し、「**OUIコードファイルをアップロードし読み込む**」ボタンをクリックします。

21. アプリ情報

本ソフトウェア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。

「メンテナンス」メニューをクリックします。



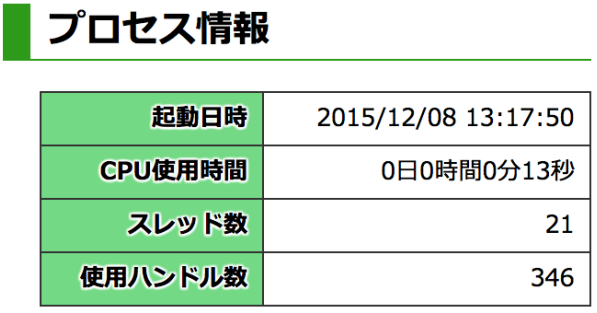
「アプリ情報」をクリックします。

21-1. バージョン情報

本ソフトウェアのバージョン番号が表示されます。

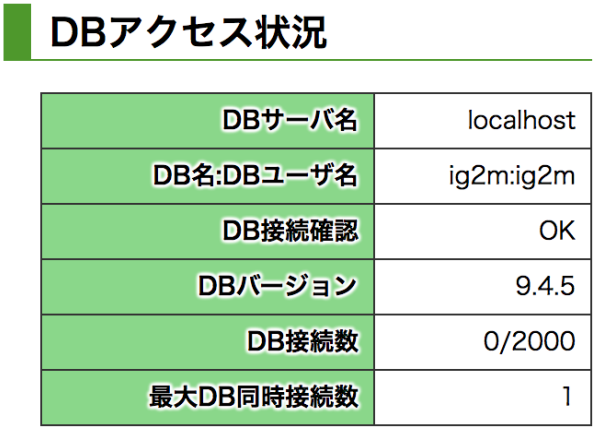
21-2. プロセス情報

本ソフトウェアの実行情報が表示されます。



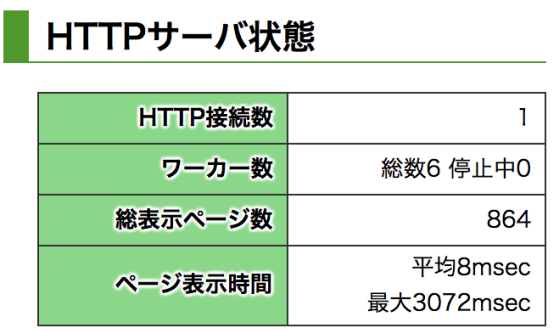
21-3. DBアクセス状況

本ソフトウェアで利用しているデータベースのアクセス状況が表示されます。
データベース関連の設定に問題がないか、確認することができます。



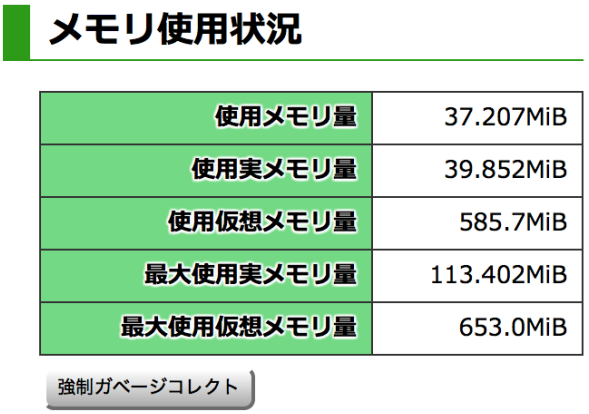
21-4. HTTPサーバ状態

本ソフトウェアで稼働しているHTTPサーバの状態が表示されます。
HTTPサーバへの接続数や表示したページの累計数、ページ表示に要した時間の平均値や最大値を確認することができます。



21-5. メモリ使用状況

本ソフトウェアのメモリ使用状況が表示されます。
「**強制ガベージコレクト**」ボタンをクリックすると、ガベージコレクトを強制実行することができます。

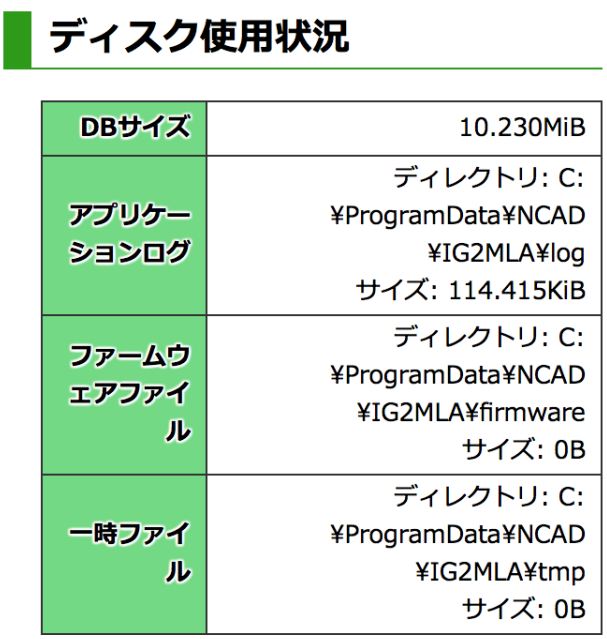


21-6. アプリケーションログ

本ソフトウェアのログのダウンロード、及びログ動作を変更することができます。
ログ出力レベルを変更することで詳細な内容を出力することが可能ですが、ストレージの使用量は増加します。
「**SQLログ出力**」で「**はい**」を選択するとログを大量に出力し、こちらも同様にストレージの使用量は増加します。

21-7. ディスク使用状況

本ソフトウェアによる各種ファイルの保存ディレクトリ、及びストレージの占有サイズを表示しています。

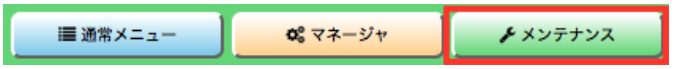


22. アプリ終了

本ソフトウェアの終了、及び再起動を実行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。

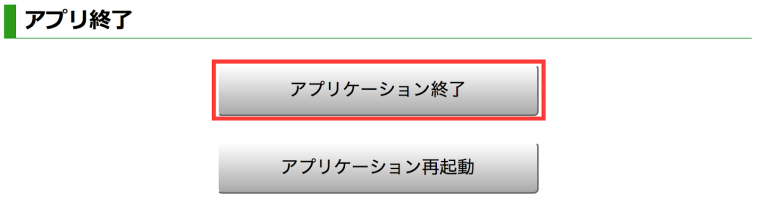
トップメニューの「**メンテナンス**」メニューをクリックします。



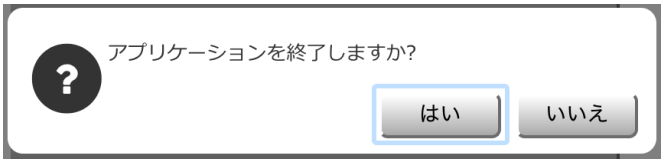
「**アプリ終了**」タブをクリックします。

22-1. アプリケーション終了

「**アプリケーション終了**」ボタンをクリックします。

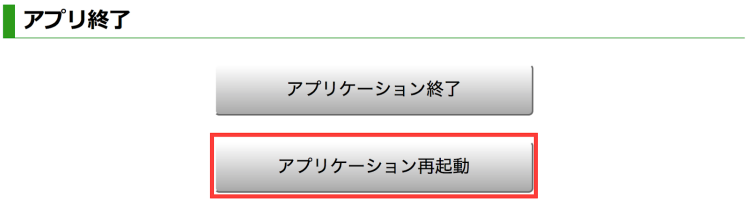


確認ダイアログが表示されるので、「**はい**」をクリックすると本ソフトウェアを終了することができます。

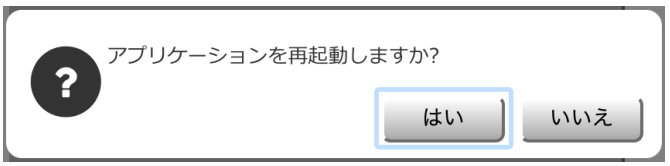


22-2. アプリケーション再起動

「**アプリケーション再起動**」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**」をクリックすると本ソフトウェアを再起動することができます。



改訂履歴

2016-03-03	初版 (v3.0)	
2016-04-14	第2版 (v3.0)	・4.3.3　管理マネージャのための設定 　マネージャアドレス変更の際に再起動が必要な旨を追記 ・4.5.4　IPアドレス重複機能 　IPv6の重複排除を行わない旨を追記 ・4.3.4　RADIUS 注意書きを加筆
2016-08-16	第3版 (v3.1)	OS検知の誤記を修正 ソフトウェアの使用許諾条件 の体裁修正 表紙のページ番号削除 USB端子についての説明体裁修正 メンテナンスと修理のためにの体裁修正 仮のVLAN設定の説明の体裁修正 リアルタイムクロックについての説明を訂正 マネージャ利用時の再起動についての説明を訂正 IPアドレス監視機能の画像を修正 排除用に本体のMACアドレスを利用の文言を修正 Ver.3.1 に対応 ・4.4　例外IPアドレス一覧の画像を範囲指定したものに変更 ・4.4.1　例外IPアドレスの登録のTIPSに範囲指定について追記 ・4.4.4　RADIUSに関する記述を削除 ・4.6.9　インスペクションに関する記述を削除 ・4.6.1　メール通知にSSLについて追記
2017-03-31	第4版 (v3.2)	登録済みPCの[全件削除]ボタン、不正接続PC一覧の[全件登録]ボタン、検知履歴の[クリア]ボタン、例外ベンダーの[全件削除]ボタンに、それぞれ”確認ウィンドウ”を追加 “機器名称設定”を追加 管理マネージャのための設定に”組織ID入力欄”を追加
2017-08-31	第5版 (v3.3)	バージョン番号の更新
2018-01-24	第6版 (v3.4)	不正検知メールの追加 排除パケットカスタマイズの追加 IPv6機能を有効にするの追加 管理マネージャ Ver3系の接続状況の追加 排除パケットの排除時MACアドレスの変更
2018-04-24	第7版 (v3.4.2)	・IG本体から発送するメールの件名のデフォルト値について設定画面に説明を追記
2018-06-08	第7版 (v3.4.3)	・20-3. OUIコードファイルのアップロードを追記 ・オペレーター設定の通知項目に端末登録を追記 ・評価版・無償版の制限事項を追記
2018-10-03	第8版 (v3.5.1)	・動作設定の「追跡時間」を「不正端末追跡時間」と「登録済み端末追跡時間」に 　分割 ・マネージャ設定に「スマート検知設定」を追記 ・端末管理の端末一覧に「スマート検知」関連のカラムの扱いについての解説を追記
2018-11-19		・スマート検知における正規表現の使用についての説明を追記
2018-12-17	第9版 (v3.5.2)	・P.39,74,78,80,88 MACアドレスがオール0とオールFを除外する説明を追記 ・P.76 端末登録申請画面と申請後画面の差し替え ・P.78 申請一覧機能の画面キャプチャを差し替えてレイアウトを変更(一括登録ボタン 　を非表示)
2019-01-21	第10版 (v3.5.3)	・P.78 申請一覧機能の画面キャプチャを差し替えてレイアウトを変更(一括登録ボタン 　を再表示)
2020-07-27	第11版	・誤植の修正

	(v3.5.4)	・P76 申請時の一括登録ボタンについて追記
2021-04-19	第12版	・誤植の修正
2021-07-21	第13版	・WEBユーザーインターフェースで使用するTCPポート番号を10080から10081に変更

IntraGuardian2+ Manager Professional
Version 3.6.6 ～

ユーザーマニュアル

2021年7月21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
https://intraguardian.jp/　　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/