不正接続検知／排除システム

IntraGuardian® 2+

スタートアップガイド

version 2.5
2015/09/14

日本シー・エー・ディー株式会社

はじめに

このたびは 不正接続検知／排除システム IntraGuardian2+（「本製品」）をお買い上げいただき、まことにありがとうございます。

・本製品をご利用の前に、本ガイドをご覧になり、正しくお使いください。
・本ガイドを大切に保存してください。
・乱丁、落丁はお取り替えいたします。
・本ガイドを万一紛失または損傷したときは、下記の製造元までご連絡ください。

ご注意

・本ガイドの内容は、将来予告なく変更することがございます。

本製品に関する最新の情報は、製品サポートサイト

http://intraguardian.jp

をご覧下さい。

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/

目次

安全上のご注意

ご使用の前に、この安全上の注意をよくお読みのうえ、正しくお使いください。

 **警告**	取扱いを誤った場合、死亡もしくは重傷を負う可能性または物的損害の発生が想定されます。

 禁止	**付属の電源アダプタ以外を使用しない** 発熱、発火、破裂、感電、けが、故障の原因になります。
 禁止	**コンセントや配線器具の定格を超える使い方や、AC100V以外で使用しない** 発熱により発火の原因になります。
 禁止	**電源コード・プラグを破損するようなことをしない** 傷んだまま使用すると発火、感電、故障の原因になります。
 指示	**電源プラグを根元まで確実に差し込む** 差し込みが不完全な場合、感電や発火の原因になります。
 禁止	**本機、電源アダプタを分解、修理、改造しない** 発熱、発火、破裂、感電、けが、故障の原因になります。
 指示	**電源プラグのほこり等は定期的にとる** プラグにほこり等がたまると、湿気等で絶縁不良となり、発火の原因になります。
 禁止	**内部に金属を入れたりしない** ショートや発熱による発火または感電の原因になります。
 禁止	**水などの液体にぬらさない** **水などの液体にぬれた状態で使用しない** ショートや発熱による発火、破裂または感電の原因になります。
 禁止	**本機、電源アダプタを落としたり、強い衝撃をあたえない** 発熱、発火、破裂、けが、故障の原因になります。
 禁止	**ぬれた手で電源プラグの抜き差しはしない** 感電の原因になります。
 指示	**次のような異常があったときは、電源プラグを抜き、使用しない** • **内部に金属や水などの液体が入ったとき** • **落下などで外装ケースが破損したとき** • **煙、異臭、異音が出たとき** そのまま使用するとショートや発熱による発火、破裂または感電の原因になります。

	**注意** 取扱いを誤った場合、傷害を負う可能性または物的損害の発生が想定されます。

 禁止	**本機、電源アダプタを異常に温度が高くなるところに置かない** 外装ケースや内部部品が劣化するほか、発火の原因になることがあります。	 禁止	**本機、電源アダプタの放熱を妨げない** 外装ケースや内部部品が劣化するほか、発火の原因になることがあります。
 禁止	**本機、電源アダプタを不安定な場所に置かない** 落下すると、けが、故障、発火の原因になることがあります。	 禁止	**本機、電源アダプタの上に物を置かない** 重量で外装ケースが変形し、内部部品の破損、故障や発火の原因になることがあります。

お願いとご注意

- 本製品に使用されているソフトウェアの無断複製・解析は禁止されております。
- 本製品に使用されている意匠、商標の無断使用は禁止されております。
- 本製品のハードウェアの転用は禁止されております。
- 本製品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でください。
- 本製品は、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。

免責事項について

・本製品の使用または使用不能から生ずる派生的または付随的な損害（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）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、当社の責に帰さない火災、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。

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。

・本製品に搭載されている不正接続検知／排除ソフトウェア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 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。
・Mac は米国 Apple Inc の米国およびその他の国における登録商標です。

ソフトウェアの使用許諾条件

日本シー・エー・ディー株式会社（以下、「日本CAD」といいます）が提供する本製品上のソフトウェア（以下、「本ソフトウェア」といいます）には、以下の条件が適用されます。お客様は、本製品を使用することにより、以下の条件を承諾したものとみなされます。

1.使用許諾

① 本ソフトウェアは、使用許諾されるものであり、販売されるものではありません。

② お客様には、本製品に組み込まれた形態で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。

③ お客様は、本ソフトウェアを改変または複製できません。本ソフトウェアをベースにしたソフトウェアを作成することもできません。

2.著作権等

① 本ソフトウェアに関するすべての権利は、日本CADおよびそのライセンサーが所有しております。

② 本ソフトウェアに関する著作権その他のいかなる知的財産もお客様に譲渡されるものではありません。

③ お客様は、本ソフトウェアおよび関連資料に使用されている著作権表示、商標その他の表示を除去できません。

3.リバースエンジニアリング

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

4.サポート契約

本ソフトウェアの更新は、別途締結される本製品のサポート契約で提供されます。

5.責任の限定

日本CAD（そのライセンサーを含む）は、本ソフトウェアの使用または使用不能から生じたお客様の損害等について一切責任を負いません。

6.輸出管理

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

7.ライセンサーの権利

お客様は、本ソフトウェアに関する日本CADのライセンサーが自己の名義で本契約書に基づき権利を行使できることを了承します。

8.管轄裁判所

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

以上

1　本製品概要

1.1　本製品について

本製品は社内ネットワークへ接続されているPCを監視し、許可なく不正に接続されたPCを自動的に検知・排除するための情報セキュリティ対策システムです。
本製品は不正に接続されたPCを発見すると、自動的に管理者に向けて警告メールを送信します。また、排除機能を有効にしておくことで、不正接続PCの通信を妨害し、社内ネットワークへのアクセスを遮断することができます。

1.2　本製品の機能

1.2.1　不正接続PC検知

本製品は社内ネットワークへ接続されている全PCの通信（ARPパケット）を監視します。したがって事前に登録されていない（接続許可を与えられていない）PCが社内ネットワークに接続されると、即座に検知することができます。
また、登録時と異なるIPアドレスを使っているPCを検知することもできます。

1.2.2　メール通知

不正接続PCを検知すると自動的に管理者に向けて警告メールを送信します。これにより管理者はいち早く不正接続PCの存在を把握することができ、社内システムの情報セキュリティ対策に絶大な効果が期待出来ます。通知できるメールアドレスは１つとなります。

1.2.3　不正接続PC排除

本製品の不正接続PC排除機能を有効にしておくことで、たとえ管理者が不在の場合であっても管理者に変わって本製品が自動的に不正接続PCを社内ネットワークから排除します。

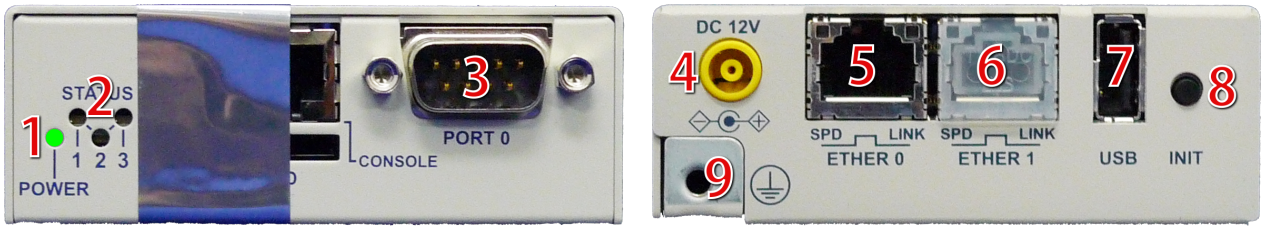
1.2.4　リモートPC起動

本製品の管理画面から、登録PCの電源を入れることができます。これにより、サーバ機等の節電運用が容易になります。（本機能を利用するためには当該PCがマジックパケットによるWake on Lan機能に対応している必要があります。）

2　ご使用の前に

本製品をご使用いただく前に把握しておいていただきたい、各部の名称や接続方法を解説します。

2.1　各部の名称



1　電源LED
2　ステータスLED（1～3）
3　シリアルコネクタ（メンテナンス用です。お使いにならないでください）
4　電源コネクタ
5　LANコネクタ
6　拡張LANコネクタ（将来の拡張用です。お使いにならないでください）
7　USBコネクタ（メンテナンス用です。お使いにならないでください）
8　初期化ボタン
9　アース

＊ 3,6,7の部分はメンテナンス、修理のために指定された技術者のみが使用する部分です。
＊ お客様がこの部分を使われて、機器の不具合が起きた場合には弊社はその不具合または不具合によって引き起こされた他の機器、システムへの不具合については一切責任を負いかねます。

2.2　準備するもの

・機器本体　（同梱されています）
・ACアダプタ　（同梱されています）
・アース線　（アースを接地する場合。お客様でご用意下さい）
・LANケーブル（ストレート）　（お客様でご用意ください）
・管理用PC　（お客様でご用意ください）

＊ 管理用PCは、イーサネットのLANポートがついていて、一般的なWebブラウザが動くPCならば何でも構いません。管理用PCには本製品専用の特別なソフトをインストールする必要はありません。

2.3　電源ケーブルの接続

付属のアダプタを電源コネクタに接続してください。本製品に電源が接続されると自動的に起動し、電源LED（緑）が点灯します。起動処理中はステータスLED1が赤く点滅しま

す。その後１分程度で起動が完了するとステータスLED1が緑色の点滅に変わり、動作可能な状態になります。

2.4　動作の終了

接続されている電源ケーブルを抜くと本製品は動作を終了します。ただし、設定情報の書き込みを行なっている間に終了してしまうと、設定情報が正しく保存されない可能性がありますので、いずれかのLEDが赤く点灯している状態で電源ケーブルを抜くことは避けてください。

2.5　リセット

初期化ボタンを５秒以上押す事で、本製品をリセットする事ができます。リセットすると全ての設定が消去され、工場出荷時の状態に戻ります。

電源を入れた状態で初期化(INIT)ボタンを5秒間押し続けると、ステータスLED3が一瞬赤く光ります。その後リセットボタンを離すと、ステータスLED3が赤く点滅し、設定初期化と再起動を行ないます。ステータスLED1が緑点滅になるまで、2分程度お待ちください。

＊ リセットボタンを10秒以上押し続けると、ステータスLEDが2回点滅し、保守作業用の特別な動作状態に入ります。万が一この保守状態になった場合は、電源ケーブルを一度抜いて、入れ直して下さい。

ご注意ください！

ステータスLED横の銀色シールは封印シールです。

シールを剥がすと保守サポートは受けられなくなります。

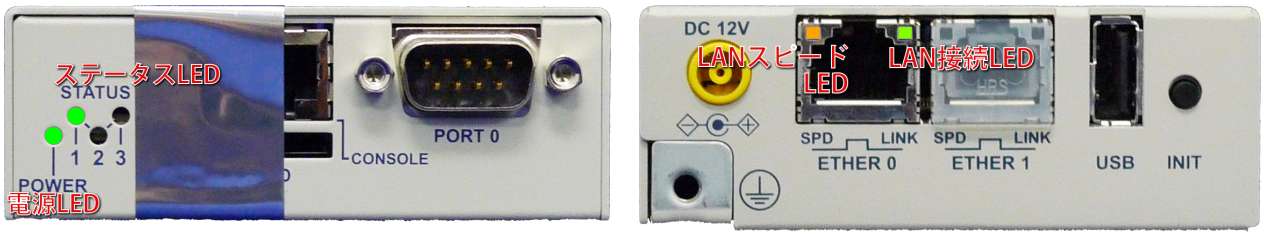
3　ネットワーク接続の設定

本製品をネットワークに接続するための設定を行ないます。

3.1　本製品の接続

本製品のLANコネクタ(ETHER　0)と管理用PCをLANケーブルで直接繋いでください。
（拡張LANコネクタ(ETHER 1)には何も接続しないでください。）
次に本製品の電源ケーブルを接続し、ステータスLED1が緑点滅になるのを待ちます。

このとき、正常な状態だと、各LEDは次のようになります。



電源LED(POWER)は緑点灯しています。
ステータスLED1は緑点滅（2回ずつ点滅）しています。（起動途中は赤点滅します。）
ステータスLED2は消灯しています。
ステータスLED3は消灯しています。（データ保存中やファームウェアアップデート中などの特殊な状態になっていない事を示します。）

LANスピードLED(SPD)は点灯しています。(1000Mbpsで接続している時には橙、100Mbpsで接続している時には緑に点灯します。接続していないか、10Mbpsで接続している時には消灯します。）
LAN接続LED(LINK)は不定期に点滅しています。（接続中は通常点灯しており、LAN上で通信が行なわれている瞬間に点滅します。）

なお、本製品のイーサネットポートは 10Mbps・100Mbps および 1000Mbps に対応しております。通信速度およびケーブルのストレート／クロス認識は自動で行なわれます。

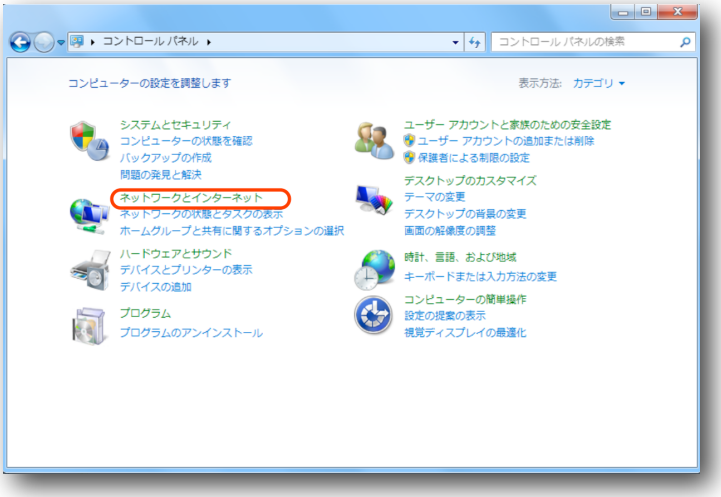
3.2　本製品の管理画面にアクセス

本製品は管理用にWebインタフェース（以下、管理画面といいます）を備えています。
ここでは、管理画面にアクセスする方法を解説します。

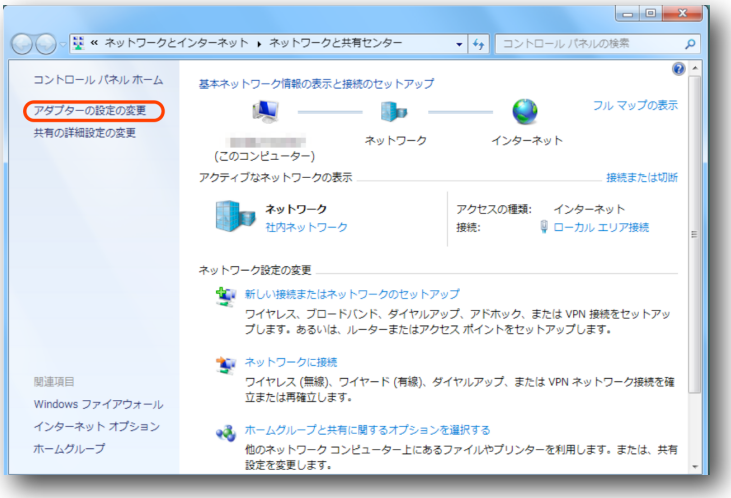
3.2.1　管理用PCのネットワーク準備 (Windows7)

本製品の初期設定をするにはPCのネットワーク設定を一時的に変更する必要があります。

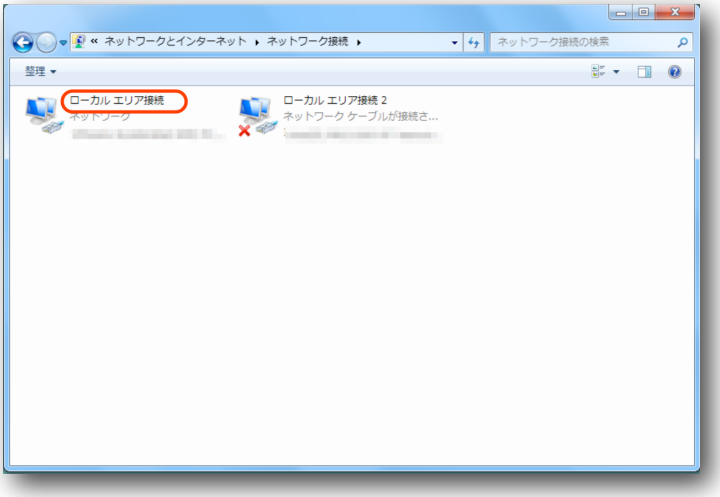
本項では、Windows7のPCのネットワーク設定についてご説明します。Mac OSX(10.9)をお使いの方はこの次の項をご覧下さい。その他のOSをお使いの場合は、OSの説明書などをご覧になって同等の設定を行なってください。
なお、ハードウェア構成によっては、本説明と異なる画面が表示されることがあります。



まず、コントロールパネルから「ネットワークとインターネット」を開いてください。

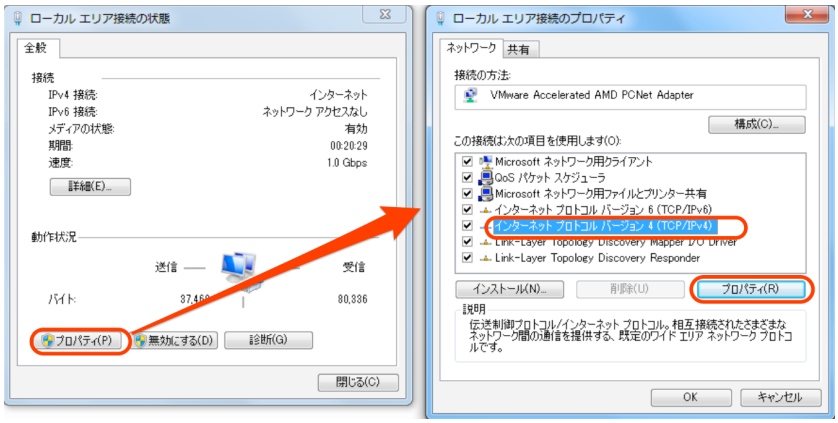


ネットワークとインターネットの画面が出たら「アダプターの設定の変更」をクリックします。

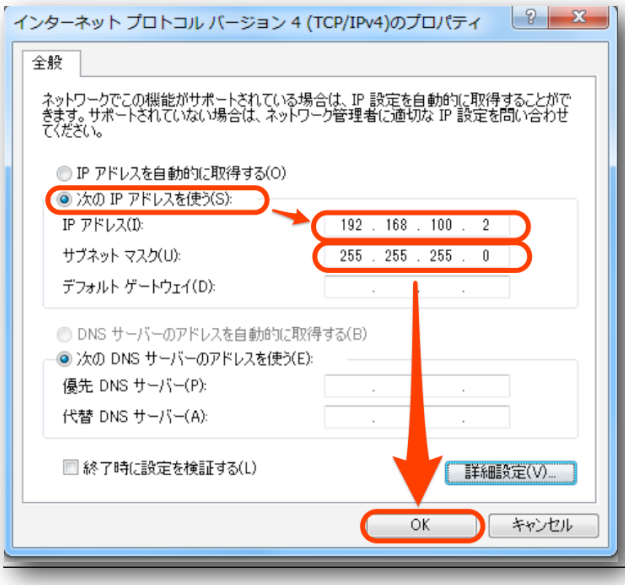


IntraGuardian2+　が接続されているネットワークアダプタをダブルクリックします。

「プロパティ」ボタンをクリックするとネットワークアダプタのプロパティのウィンドウが開きますので、「インターネットプロトコルバージョン4 (TCP/IPv4)」のプロパティを開いてください。



「インターネットプロトコルバージョン4(TCP/IPv4)のプロパティ」ウィンドウが開きますので、「次のIPアドレスを使う」を選択し、IPアドレス欄には「192.168.100.2」、サブネットマスク欄には「255.255.255.0」を入力します。IPアドレスとサブネットマスクを入力したら、「OK」ボタンをクリックします。



これで、管理用PCのネットワーク準備は完了です。

3.2.2　管理用PCのネットワーク準備 (Mac OSX)

本項では、Mac OSX (10.9 Mavericks) のネットワーク設定についてご説明します。
なお、ハードウェア構成によっては、本説明と異なる画面が表示されることがあります。

システム環境設定を開き、「ネットワーク」をクリックします。

IntraGuardian2+ を接続しているネットワークインタフェースを選択し、IPv4の設定を「手入力」、IPアドレスを「192.168.100.2」、サブネットマスクを「255.255.255.0」と入力します。
入力したら「適用」をクリックします。

これで管理用PCのネットワーク準備は完了です。

3.2.3　Webブラウザの起動

管理画面にアクセスするために、管理用PCでWebブラウザ（以下、ブラウザ）を起動します。

＊ 各画面のスクリーンショットにつきまして、お使いのブラウザ等によっては実際の表示と異なる場合がございます。

3.2.4　本製品の初期アドレスを入力

本製品には出荷時に固定の初期アドレスが設定されています。
ブラウザのアドレス欄に以下の初期アドレスを入力して本製品にアクセスします。

初期アドレス	http://192.168.100.1

次のようなログイン画面がブラウザに表示されます。

「ユーザー名」と「パスワード」を入力して、[ログイン] ボタンをクリックして管理画面にログインします。ユーザー名とパスワードは出荷時に以下の通りに設定されています。

ユーザー名	admin
パスワード	admin

3.2.5　英語での利用

ログインをする際に、言語メニューで「English」を選択すると、以降の画面が全て英語での表記になります。（使用できる機能に違いはありません。）

また、ご利用のブラウザの設定で、日本語よりも英語を優先するようになっている場合には、ログイン画面は英語で表示されます。この場合、Languageメニューで「日本語」を選択してログインすることにより、全ての操作を日本語画面で行うことができます。

3.3　メニュー項目

管理画面の左側には常にメニューが表示されます。

本製品を初めて設置する場合、まず設置設定でIPアドレスなどを設定してから運用環境のネットワークに接続し、他の設定項目を調整するという流れになります。

3.4　設置設定

本製品を社内ネットワークに設置するための設定を行ないます。

3.4.1　ネットワーク設定

本製品には出荷状態で固定の初期IPアドレスが設定されていますが、ご使用の環境に合わせて変更する必要があります。
メニューから「設置設定」をクリックすると、本製品のIPアドレスを設定する画面が表示されます。各項目の入力内容は以下の通りです。

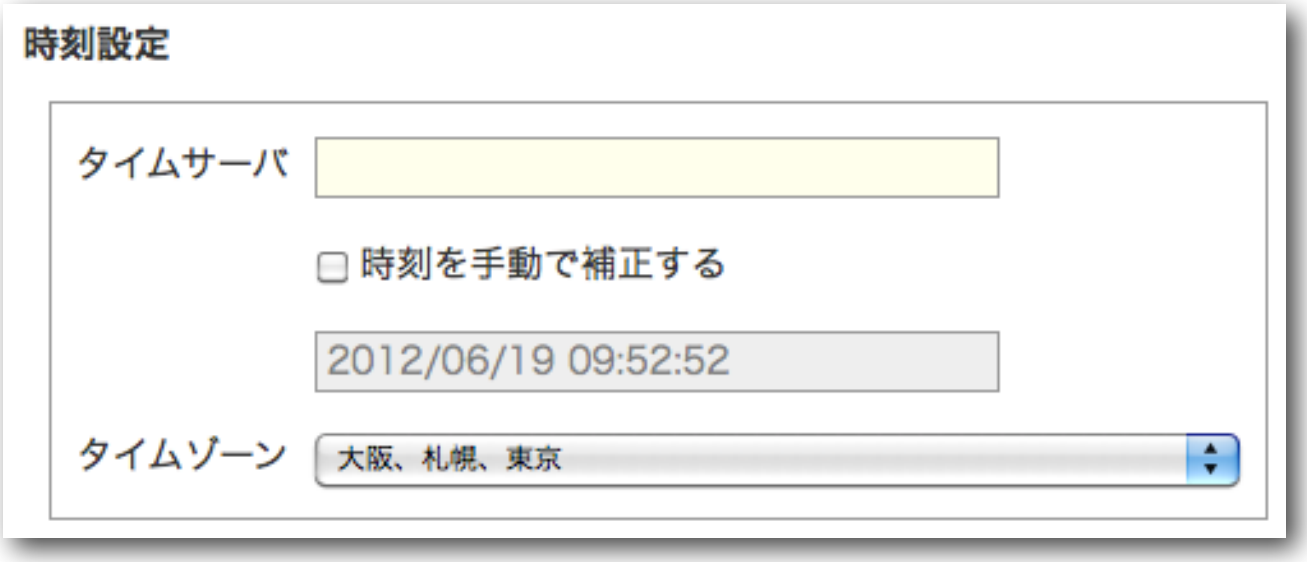
IPアドレス	本製品に割り当てるIPアドレス
ネットマスク	設置するネットワークのネットマスク
ゲートウェイ	設置するネットワークのデフォルトゲートウェイのIPアドレス
定期確認を実施する	デフォルトルートと通信できるかどうかを定期的にチェックする場合にはチェックマークをつける
ネームサーバ	名前解決の際に利用するネームサーバ（DNSサーバ）のIPアドレス

＊ ネームサーバは2つまで入力する事ができます。ネームサーバが利用できない場合には2つとも空欄にしても構いませんが、メール送信サーバやタイムサーバなどをホスト名で指定することができなくなります。また、DNSによる名前解決機能が動作しなくなります。

＊ 「定期確認を実施する」にチェックマークを入れておくと、約1分に1回の頻度で、デフォルトルートで指定されるIPアドレスにPING要求（ICMP要求）を出します。この応答が無い場合には、本装置のネットワークインターフェースを初期化し直します。
これは、本装置に異常なパケットが送りつけられるなどの要因により、万が一ネットワークインターフェースが誤動作しても自動復旧するようにするための機能です。

3.4.2　時刻設定

本製品の時刻を設定します。タイムサーバを指定すると自動で時刻が同期されますが、手動で設定することも可能です。なお、本製品はリアルタイムクロックを搭載しておりますが、月に数分程度の誤差が生じる可能性があります。正確な時刻情報を得るためにはタイムサーバの指定をします。



タイムサーバ	本製品の時刻を同期するためのタイムサーバ（NTPサーバ）のアドレス IPアドレスかドメイン名で入力できます。 ＊ 時刻同期は本設置設定を確定した時、起動時、および起動後約8時間毎に行ないます。
時刻を手動で補正する	この項目をチェックすると、時刻を手動設定することができます。NTPサーバが利用できない環境に設置する際にはご利用ください。 入力欄には「YYYY/MM/DD HH:MM:SS」の形式で現在日時を入力してください。
タイムゾーン	設置場所のタイムゾーンを選択してください。タイムゾーンの設定は**IntraGuardian2+の再起動後**に有効になります。

TIPS:

自社内にタイムサーバがある場合には、できるだけ自社内のタイムサーバを指定してください。
社内にタイムサーバが無い場合には、”ntp.nict.jp”などの公開NTPサーバをご利用ください。なお、ntp.nict.jp のご利用に際しては、独立行政法人 情報通信研究機構の日本標準時プロジェクトのページ http://www2.nict.go.jp/aeri/sts/tsp/PubNtp/index.html をご覧下さい。

3.4.3　管理マネージャのための設定

IntraGuardian2 Manager を利用する予定の場合には、「管理マネージャを使用する」のチェックマークをつけ、「管理マネージャアドレス」欄に Manager のIPアドレスを入力してください。管理マネージャアドレスは最大で3件指定可能です。

TIPS:

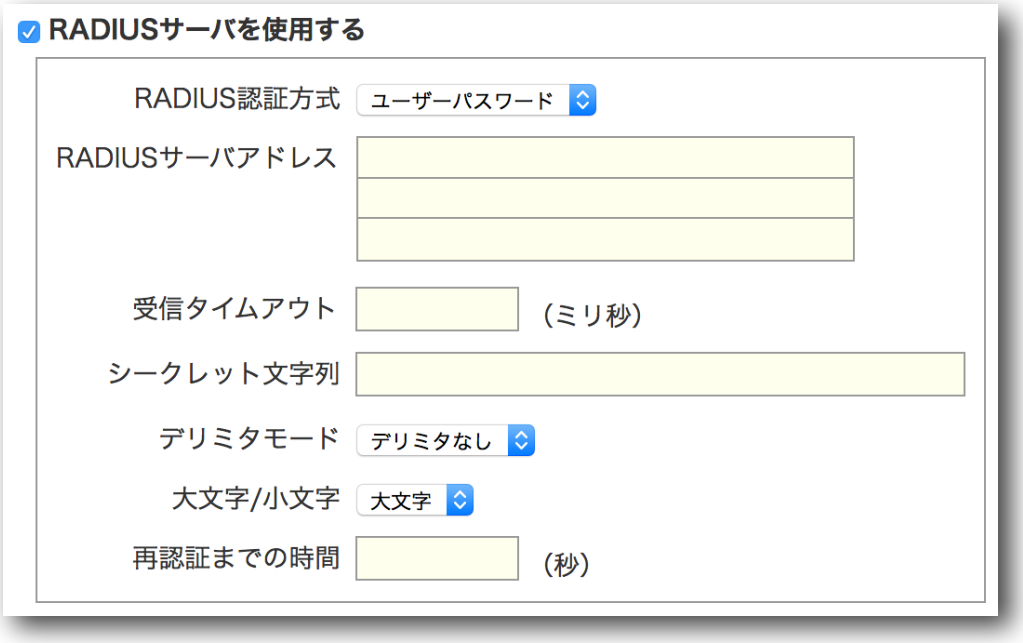
データベース保存場所とは、登録PC一覧の保存場所のことです。
この設定は、IntraGuardian2 Manager の管理画面からのみ変更ができるようになっています。

管理マネージャ種別の表示はご使用のモデル・バージョンにより異なる場合がございます。また、複数選択可能な場合もございますので、設定方法につきましては管理マネージャメーカにお問い合わせください。

3.4.4　RADIUSサーバを使用する

不正接続端末を検知した際の許可認証にRADIUSを利用する設定をします。各RADIUSの設定は以下の通りです。

※RADIUS認証データは、ユーザIDとパスワードにそれぞれ許可すべきMACアドレスとしてください。



RADIUS認証方式	RADIUS認証方式に、「ユーザパスワード」認証、または「CHAP」認証の設定をします。
RADIUS サーバアドレス	RADIUSサーバのアドレスを指定します。最大３つまで指定可能です。
受信タイムアウト	RADIUSサーバへ問い合わせ時のタイムアウト値を設定します。 ※500～5000までで指定してください。
シークレット文字列	RADIUSのシークレットを指定します。
デリミタモード	MACアドレスのデリミタを指定します。
大文字/小文字	MACアドレスの文字種（大文字・小文字）を指定します。 ※大文字、小文字の併用はできません。
再認証までの時間	RADIUS認証で接続許可後、再度認証するまでの時間を指定します。 ※1～3600までで指定してください。

3.4.5　設置設定の確定

これらの項目に入力を終えたら、[確定] ボタンをクリックしてください。
設定変更に成功すると以下のメッセージが表示されます。

この段階で本製品のIPアドレスは変更されています。
今後管理画面にアクセスする際は、画面に表示されているアドレスにアクセスする事になるので忘れないようにメモしておいてください。
万が一忘れてしまった場合は、【2.5　リセット】の説明に従って本製品を工場出荷状態に初期化し、はじめから作業を行なってください。

3.4.6　本製品の設置

設置設定の変更が完了したら本製品を実際に運用するネットワークに設置してください。

TIPS:

起動直後のネットワーク通信が安定して行なえるように、LANケーブルを先にさしてネットワークに接続してから、本製品の電源ケーブルを差し込むようにしてください。

3.4.7　管理用PCの設置

本製品の設置が終わったら、管理用PCの設置を行ないます。【3.2.1　管理用PCのネットワーク準備】で変更したPCの設定を元に戻して、本製品と同じネットワークに接続してください。

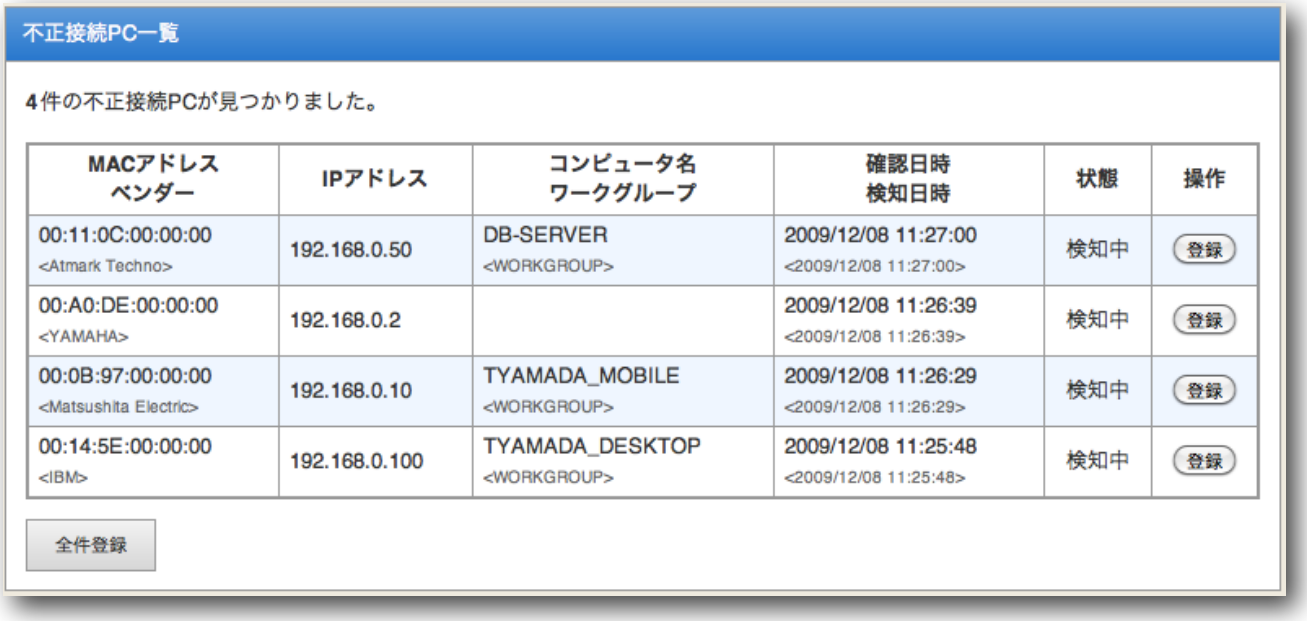
接続完了後、本製品の新しいアドレスとして先ほど設定したアドレスにアクセスして管理画面にログインしてください。

管理画面のアドレス	http://IntraGuardian2+のIPアドレス

3.5　既存PCの登録

運用を開始する前に、現在稼動中の既存PCを、本製品へ登録します。

(1) メニューから「不正接続PC一覧」を押下します。
(2) ネットワーク内の既存PCが不正接続PCとして一覧表示されます。
＊ クラスCのネットワークの場合、およそ30秒でセグメント内のPCを全て検知します。
(3) 既存PCを個別に登録する場合は、登録するPC欄右端の [登録] ボタンを押下します。
全件一括で登録する場合には、画面最下部の [全件登録] ボタンを押下します。
(4) 対象のPCが本製品に登録され、不正接続PC一覧から消去されます。



TIPS:

既存PCの一括登録は、【4.7　バックアップ / 復元】の手順でCSVファイルをインポートして行う事も可能です。

3.6　動作設定

本製品の検知/排除機能に関する動作を、導入するネットワークに合わせて調整します。

3.6.1　動作設定

(1) メニューから「動作設定」を押下します。
(2) 動作設定画面が表示されるので、下表の項目を入力します。
(3) 画面最下部にある [確定] ボタンを押下すると、設定が変更/反映されます。

追跡時間（秒）	不正接続PC一覧から検知履歴に移動するまでの時間
動作モード	検知：（メール通知）のみ行う 排除：検知および排除（通信排除）を行う 保留：検知後、保留時間経過後に排除へ移行する
保留時間（分）	検知後、排除へ移行するまでの保留時間（保留のみ）

＊ 動作モードの変更は、必ず既存PCの登録を済ませてから行なって下さい。
＊ 万が一、管理用PCを登録せずに動作モードを「排除」に設定すると、管理用PCから本製品にアクセスできなくなることがあり、設定を変更する事ができなくなる可能性があります。
＊ 管理用PCから本製品にアクセスする際にルーターを経由している場合には、必ずルーターを本製品に登録してください。

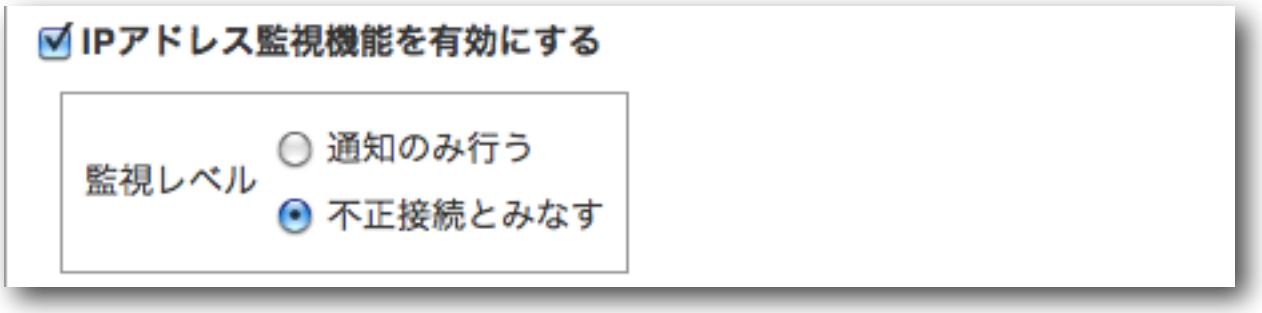
TIPS:

本製品が検知したPCは、それが登録されていないものである場合には「不正接続PC一覧」に掲載されます。（動作モードが「排除」の場合には、同時に当該PCの通信を妨害するパケットを出し始めます。）
引き続き同じPCが検知され続ければ、その「確認日時」が更新されてゆきます。

本製品は、最新の確認日時から「追跡時間」以上経過したPCの記録があれば、それを「不正接続PC一覧」から「検知履歴」に移します。
なお、動作モードが「保留」の場合には、初めてPCが検知されたときから「保留時間」以上経過した場合に、排除行動を始めます。

3.6.2 IPアドレス監視機能

LAN上のPCに固定IPを割り当てて運用している場合などには、登録されているPCでも正しいIPアドレスを使っていない場合には不正接続と見なしたい場合があります。
このような場合には、[IPアドレス監視機能を有効にする] をチェックしてください。



[IPアドレス監視機能を有効にする] 場合には、監視レベルとして [通知のみ行う] か [不正接続とみなす] を選択してください。
[通知のみ行う] の場合には、登録されているIPアドレスと異なるIPアドレスで動作しているPCを発見した場合にメールを発送します。（ただし、[通知設定] 画面で [IPアドレスの変化を通知する] がチェックされていない場合には、メールは送られません。）
[不正接続とみなす] の場合には、登録されているIPアドレスと異なるIPアドレスで動作しているPCは不正接続PCとして扱います。（動作モードが [排除] ならば、排除行動をとります。）

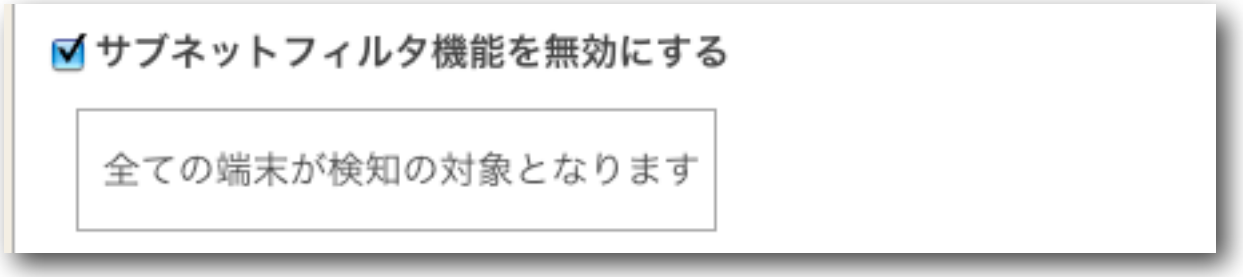
- [通知のみ行う] をチェックしていても、通知設定画面で [メール通知を有効にする] にチェックが付いていない場合や、[IPアドレスの変化を通知する] にチェックが付いていない場合には、メール通知は行なわれません。
- 画面最下部の [確定] ボタンを押下したタイミングで反映されます。

3.6.3　サブネットフィルタ機能

本製品には、自身と同一サブネット内のPCのみを検知するサブネットフィルタ機能があります。サブネットフィルタ機能を無効にすることで、同一セグメント内のPCはネットワークアドレスの如何に関わらず全て検知することが可能になります。（ただし、スイッチングハブやルーターなどにより本製品に当該PCのパケットが到達しない場合には検知はできません。）
本機能は、出荷時は有効に設定されていますので、本製品と同じネットワークアドレスを持つPCのみを検知する状態になっています。

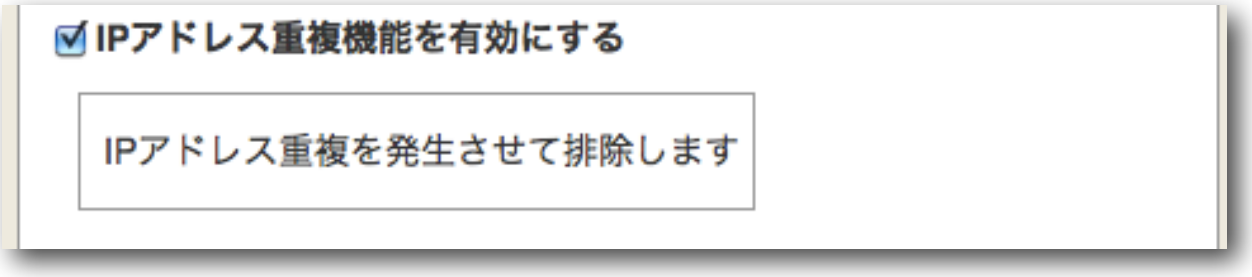
[サブネットフィルタ機能を無効にする]　をチェックまたは解除することでサブネットフィルタ機能の 有効 / 無効 を切り替えます。

＊ 画面最下部の [確定] ボタンを押下したタイミングで反映されます。



3.6.4　IPアドレス重複機能

本機能は、不正接続PCの排除を行う際に、不正接続PCのIPアドレスが重複するようなパケットを送信し、排除を行う機能です。
DHCPサーバご利用の環境では問題が発生する可能性があるため、この機能をOFFにすることをお勧め致します。



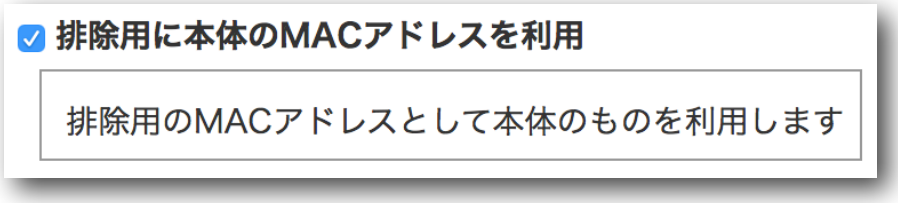
TIPS:

IntraGuardian2+は排除を行う際にIPアドレスの重複を発生させるため、DHCPサーバご利用の環境ではIPアドレスが枯渇する（IPアドレスが払い出せなくなる）場合がございます。
この問題は、IPアドレスの重複を検出した排除クライアントが、DHCPサーバにDECLINEメッセージを送信し受信したDHCPサーバは、そのIPアドレスを「BAD ADDRESS」(利用出来ないアドレス)としてマークし以降払い出しに使用しなくなるため発生致します。

3.6.5　排除用に本体のMACアドレスを利用

本機能を有効にすると排除する際に利用するMACアドレスが本体MACアドレスを利用し排除します。

※本機能を無効にした場合は従来の動き通り「CC:AA:DD:CC:AA:DD」で排除されます。



3.6.6　DNSによるコンピュータ名の取得機能

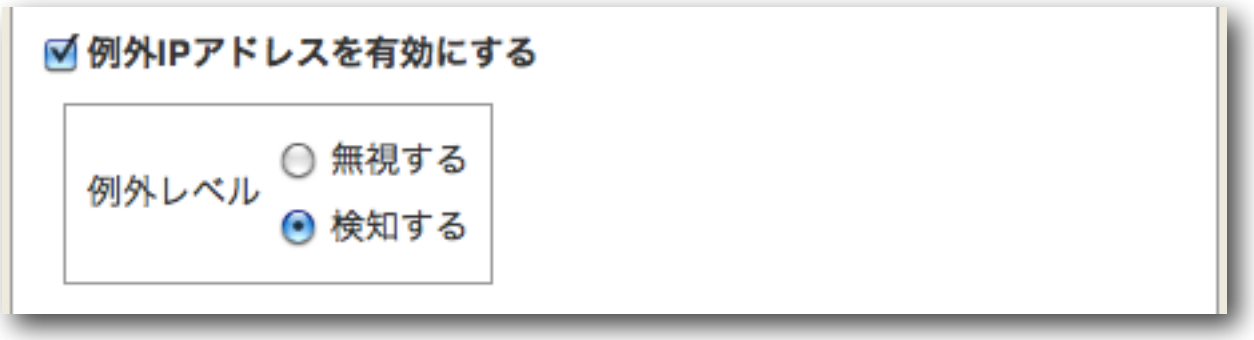
本製品はネットワーク上に存在していることを検知したPCの名前を、NetBIOS（Windows共有）プロトコルを使って獲得しようとします。このとき、DNSでも名前解決を試みるかどうかを設定します。

DNSによるコンピュータ名の取得を有効にする場合は、NetBIOSで見つけた名前とDNSで見つけた名前のどちらを優先して使うかを選択します。

＊ DNSでコンピュータ名を取得した時は、ワークグループ名は空欄になります。

3.6.7　例外IPアドレス登録機能

あらかじめ本製品に登録してあるIPアドレスの機器については、不正端末として処理しないようにする機能です。冗長化などの都合でしばしば機器本体が入れ替わる（あるIPアドレスに対応するMACアドレスが時々変わる）サーバなどがある場合に、有効にしてお使いください。



例外IPアドレスを有効にする場合は、例外レベルも指定します。例外レベルが「無視する」の場合、当該IPアドレスを持つ機器を検知しても、不正接続PC一覧には表示されません。例外レベルが「検知する」の場合、当該IPアドレスを持つ機器は不正接続PC一覧に表示されますが、排除対象となる事はありません。（ただし、当該機器のMACアドレスが登録済みPC一覧にある場合には、不正接続PC一覧には表示されません。）

＊ 動作設定画面で本機能を有効にしても、例外IPアドレス登録をしていない場合には本機能は無効になります。例外IPアドレスの登録については、【4.4 例外IPアドレス一覧】をご覧下さい。

TIPS:

PCを含む一般的なネットワーク機器では、IPアドレスの詐称はごく簡単にできてしまうため、本機能を有効にすると不正端末を見逃してしまう可能性が生まれてしまいます。

冗長化構成によりあらかじめ代替機となる機器のMACアドレスが分かっている場合、それを登録済みPC一覧に登録しておき、本機能は無効にしておくという運用をお勧めします。

ルーターなどの故障修理時に、どのようなMACアドレスの機器が代替機になるかわからないという場合にのみ、本機能をお使いください。

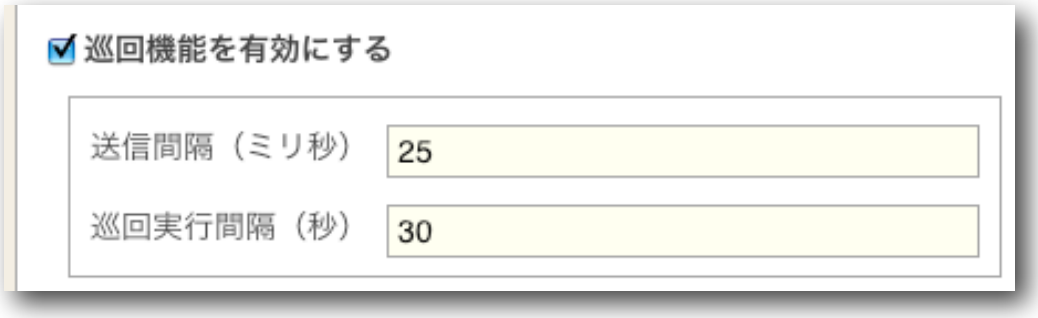
3.6.8　巡回機能

本製品には、不正接続PCを確実に検知するために、セグメント内を定期的に巡回する機能があります。本機能は、出荷時は有効に設定されています。

(1) [巡回機能を有効にする] をチェックまたは解除することで、巡回機能の 有効 / 無効を切り替えます。

＊ 画面最下部の [確定] ボタンを押下したタイミングで反映されます。

(2) 巡回機能を有効にする場合には、合わせて下表の項目を設定します。



送信間隔（ミリ秒）	ARPリクエストパケットの送信間隔 ＊ 極端に小さな値はネットワークへの負担を高めます。5ミリ秒以上を設定してください。
巡回実行間隔（秒）	巡回を終えた後に次の巡回を開始するまでの間隔

TIPS:

一般的なスイッチングハブを用いたネットワーク構成の場合、ブロードキャストパケットや本製品宛のパケット以外は本製品に届かないため、本製品で機器の存在を検出することができません。
ネットワーク帯域が著しく小さいなどの特別な理由が無い限り、巡回機能は常に有効にしてお使いいただく事を強くお勧めします。

TIPS:

本製品は、送信間隔で指定した時間間隔でサブネット内の全IPアドレスに対してARP要求パケットを発行します。全IPに対する発行が終わったら、巡回実行間隔で指定した時間だけ休み、再びARP要求パケットの送信を始めます。
つまり、クラスCのネットワークで上記の設定をした場合、
254×25msec+30sec = 36.35sec
毎にサブネット内の全IPアドレスの検査を行う事になります。
クラスBなどの大きなネットワークを使っている場合には、この検査周期が追跡時間で設定した時間よりも大きくならないように注意してください。

3.6.9　インスペクション機能を有効にする

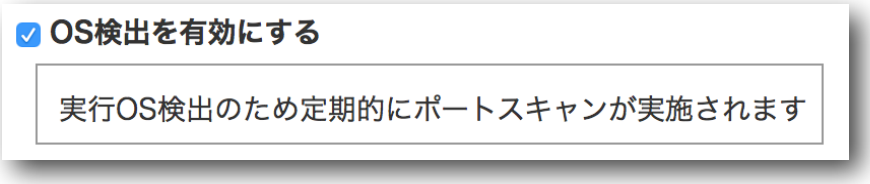
インスペクション機能は、不正と検知した端末の指定したポート番号と通信し、許可条件とマッチするかどうかを判別する機能です。
他社システムのエージェントと連携し、本製品の許可端末として扱うかどうかを判別する場合にお使いください。

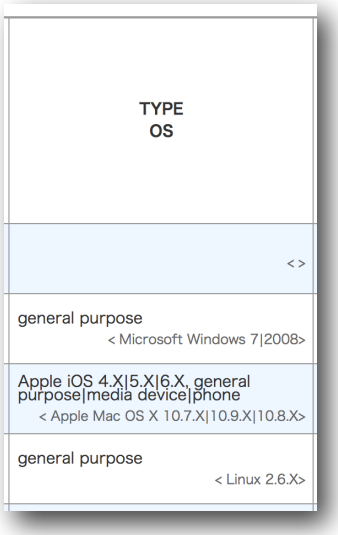
※インスペクション機能により許可された端末は登録済みPC一覧には、+付きの有効期限付きで許可されます。
※インスペクション機能により許可された端末を削除することはできません。再起動により表示からなくなります。
※許可端末かどうかの問い合わせ中は端末排除が行われませんのでご注意ください。

ポート番号	不正接続かどうか判断するためのポート番号(TCP)を指定します。
送信電文	指定したポート番号に接続した際に送信する文字列を指定します。
受信電文	送信結果の条件を指定できます。正規表現で指定可能です。
応答待ち時間（ミリ秒）	送信電文送信後の応答待ち時間を指定します。
最大確認回数	電文送信の送信確認回数を指定します。
許可時間（分）	受信電文に一致し、許可端末だった際に接続許可される時間を指定します。指定時間後、再度問題端末に許可端末かの確認を行います。

3.6.10　OS検出を有効にする

OS検出を有効にすると、登録済みPC一覧にOSの種類が表示されるようになります。
※nmapのポートスキャンによりOS検出を実施しますので、多量のCPUパワーを消費し、なおかつ対象クライアントにはセキュリティ攻撃を受けたような痕跡が残ります。これらの意味がわかる場合にのみご利用ください。




TYPE
OS
< >
general purpose
< Microsoft Windows 7|2008>
Apple iOS 4.X|5.X|6.X, general purpose|media device|phone
< Apple Mac OS X 10.7.X|10.9.X|10.8.X>
general purpose
< Linux 2.6.X>

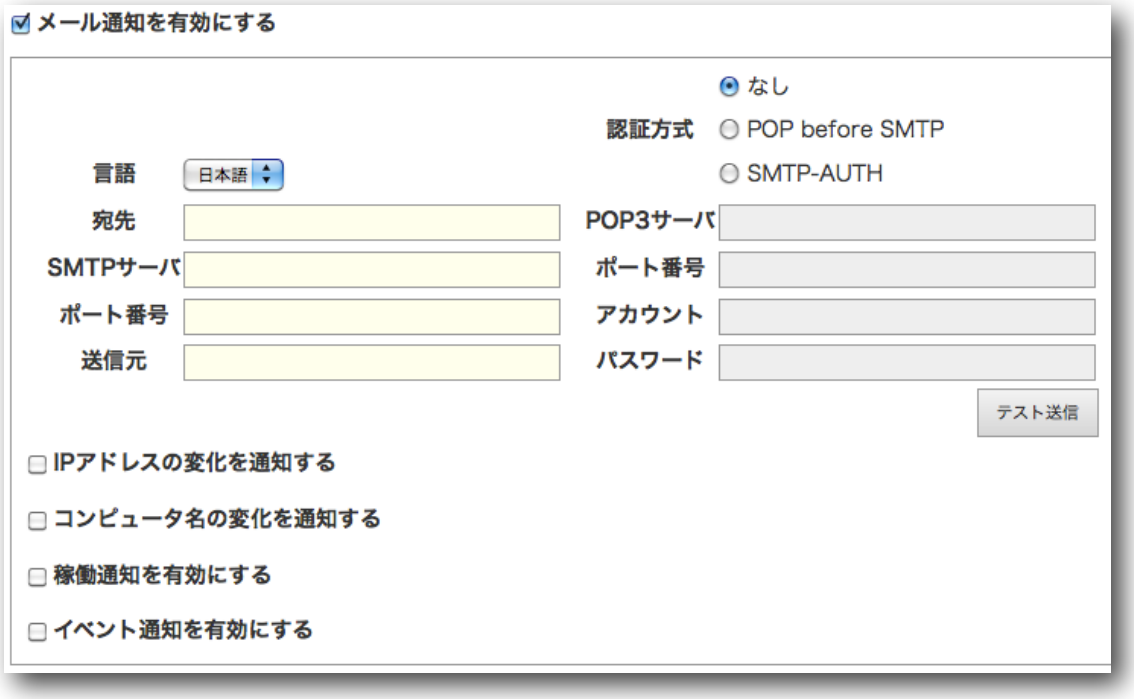
3.7　通知設定

本製品からの通知を受け取るための設定を行ないます。

3.7.1　メール通知

本製品の配信するメール通知に関する設定を行ないます。

(1) メニューから「通知設定」を押します。



(2) [メール通知を有効にする] をチェックまたは解除することで、メール通知機能の 有効 / 無効 を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(3) メール通知機能を有効にする場合には、あわせて下表の項目を設定します。

言語	メール文に用いる言語
宛先	メールを配信する際の宛先のメールアドレス
SMTPサーバ	メール配信に利用するSMTPサーバのアドレス
ポート番号	SMTPサーバで使用するポート番号。(通常25)
送信元	通知メールを配信する際の送信元メールアドレス
認証方式	メール配信に利用するSMTPサーバの認証方式
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
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(通常110)
アカウント	認証に使うユーザーアカウント
パスワード	認証に使うパスワード

宛先、SMTPサーバ、ポート番号、送信元と認証方式を設定した後で、[テスト送信] ボタンを押下すると、テストメールが宛先に送信されます。設定に誤りが無いかどうかを確認する際にご利用ください。

3.7.2 IPアドレスの変化通知

登録PCのIPアドレスが変化したものを発見したときにメールで通知します。

(1) [IPアドレスの変化を通知する] をチェックまたは解除する事で、IPアドレス変化通知の有効／無効を切り替えます。

＊ 本設定項目にチェックをつけても、動作設定画面の [IPアドレス監視機能を有効にする] がチェックされていないときには、メール通知は行なわれません。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) 通知を有効にする場合には、あわせてメールの件名を設定します。

TIPS:

DHCPを利用している場合、PCがネットワークに接続し直すとIPアドレスが異なる状態になって、本機能によりメールが発送されることがあります。
また、セグメント内のいずれかのPCが、1つのネットワークデバイス(NIC)に複数のIPアドレスを割り当てる機能（IP aliasing等）を使っている場合、頻繁にIPアドレスの変化が検知されて多くのメールが発送されます。

TIPS:

特定の登録PCだけはIPアドレス変化の通知を行ないたくない、という場合には、当該PCの登録IPアドレスを空欄にしてください。詳しくは、【4.1.1　新しいPCの登録】をご覧下さい。

3.7.3　コンピュータ名の変化通知

コンピュータ名が変化したPCを発見したときにメールで通知します。

(1) [コンピュータ名の変化を通知する]　をチェックまたは解除する事で、コンピュータ名変化通知の有効／無効を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) 通知を有効にする場合には、あわせてメールの件名を設定します。

TIPS:

コンピュータ名は、Windowsネットワーク(NetBIOS)の名称、またはDNSの名称です。

3.7.4　稼働通知

本製品が正常に稼働していることを定期的にメールで通知します。

(1) [稼働通知を有効にする]　をチェックまたは解除することで、稼働通知の有効／無効を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) 稼働通知を有効にする場合には、あわせて下表の項目を設定します。

メール件名	稼働通知を配信する際のメール件名
通知間隔	稼働通知を配信する間隔 ＊ 毎日または毎時の単位で指定可能

TIPS:

本製品が「稼働しなくなった」時に通知メールを受け取りたい場合には、IntraGuardian2 Manager をご利用ください。

TIPS:

稼働通知で指定する通知間隔は、メールの稼働通知の通知間隔指定と連動します。メールの稼働通知間隔とSNMPトラップの稼働通知間隔を別々に指定することはできません。

3.7.5　イベント通知

本製品の起動やネットワーク接続などのイベントをメールで通知します。

(1) [イベント通知を有効にする] をチェックまたは解除することで、稼働通知の 有効 / 無効 を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) イベント通知を有効にする場合には、あわせてメールの件名を設定します。

TIPS:

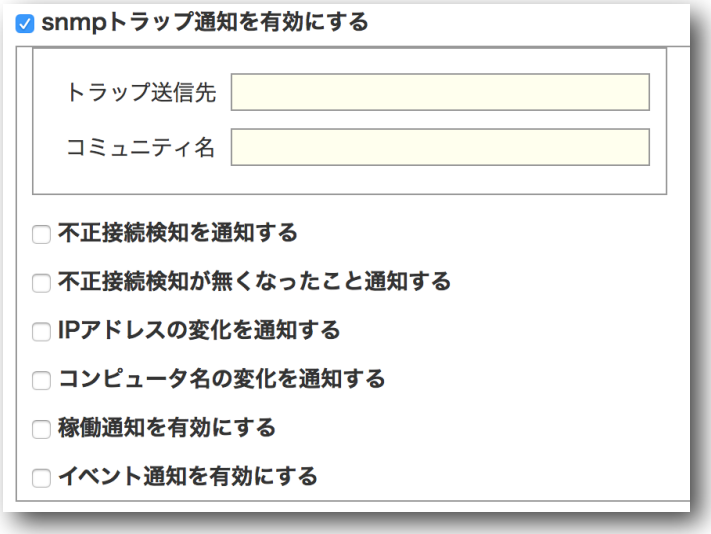
イベント通知を有効にすると、次の内容のメールが送信されます。

- 「IntraGuardian2が起動しました」
- 「IntraGuardian2がネットワークに接続されました。」

3.7.6　SNMPトラップ通知

不正接続を検知した場合等のSNMPトラップ通知の設定を行います。

(1) [snmpトラップ通知を有効にする] をチェックまたは解除することで、稼働通知の 有効 / 無効 を切り替えます。



(2) トラップ送信先のアドレスとコミュニティ名を指定し、次に通知を受けたいイベントを選択します。

3.7.7　不正接続検知を通知する

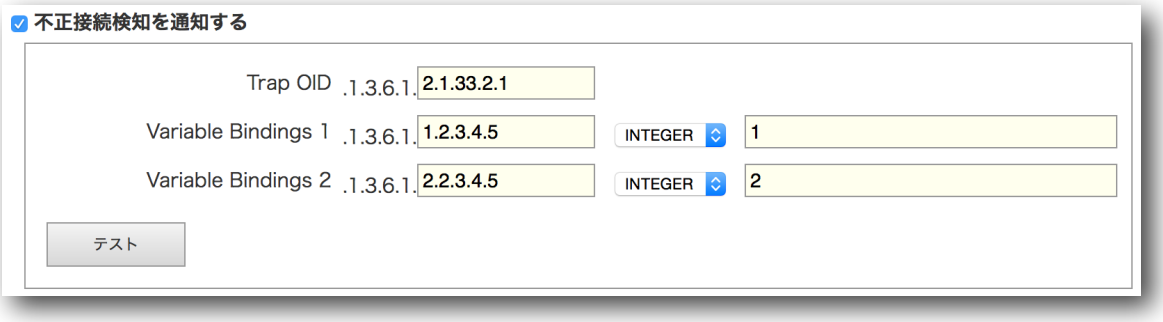
IntraGuardian2+が不正接続を検知した場合にSNMPトラップを送信します。

※Variable BindingsはIG2-03PL, IG2EX-03-08(24)VLのみの機能です。

(1) [不正接続検知を通知する] をチェックまたは解除することで、通知の 有効 / 無効 を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) 通知を有効にする場合には、あわせてOIDを設定します。



TIPS:

[テスト]ボタンを押すと、指定の送信先に入力したOIDのSNMPトラップが送信されます。

3.7.8　不正接続検知が無くなったことを通知する

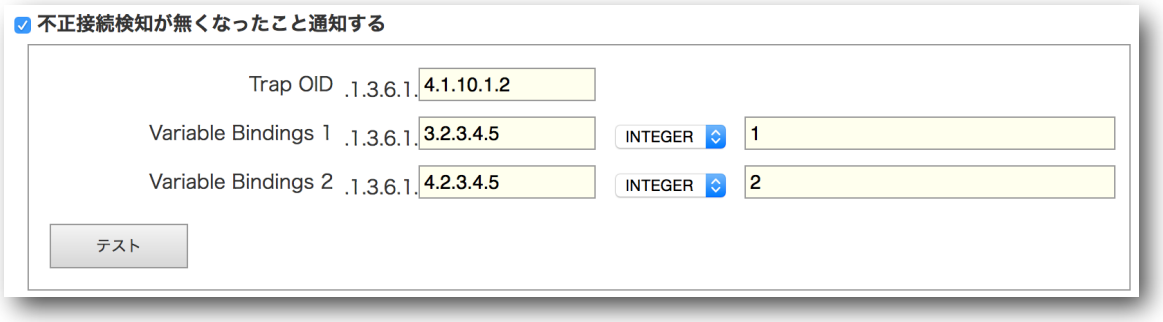
IntraGuardian2+が不正接続を検知しなくなった場合にSNMPトラップを送信します。

※Variable BindingsはIG2-03PL, IG2EX-03-08(24)VLのみの機能です。

(1) [不正接続検知がなくなったことを通知する] をチェックまたは解除することで、通知の 有効 / 無効 を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) 通知を有効にする場合には、あわせてOIDを設定します。



3.7.9　IPアドレスの変化を通知する

IntraGuardian2+が登録機器のIPアドレス変化を検知した場合にSNMPトラップを送信します。

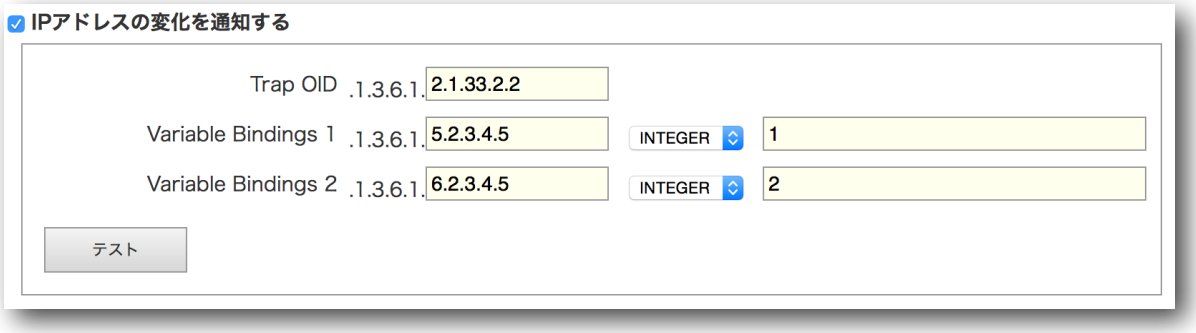
※Variable BindingsはIG2-03PL, IG2EX-03-08(24)VLのみの機能です。

(1) [IPアドレスの変化を通知する] をチェックまたは解除することで、通知の 有効 / 無効 を切り替えます。

＊ 本設定項目にチェックをつけても、動作設定画面の [IPアドレス監視機能を有効にする] がチェックされていないときには、通知は行なわれません。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) 通知を有効にする場合には、あわせてOIDを設定します。



3.7.10　コンピュータ名の変化を通知する

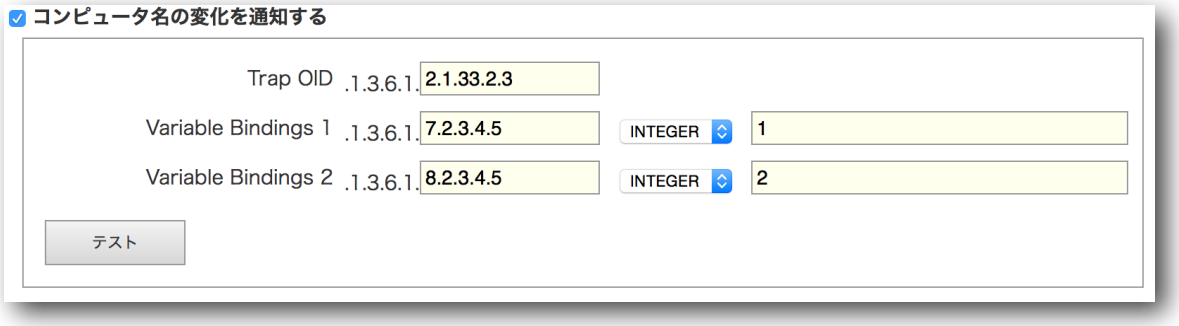
IntraGuardian2+がコンピュータ名が変化したPCを発見したときにSNMPトラップを送信します。

※Variable BindingsはIG2-03PL, IG2EX-03-08(24)VLのみの機能です。

(1) [コンピュータ名の変化を通知する] をチェックまたは解除することで、通知の 有効 / 無効 を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) 通知を有効にする場合には、あわせてOIDを設定します。



3.7.11　稼働通知を有効にする

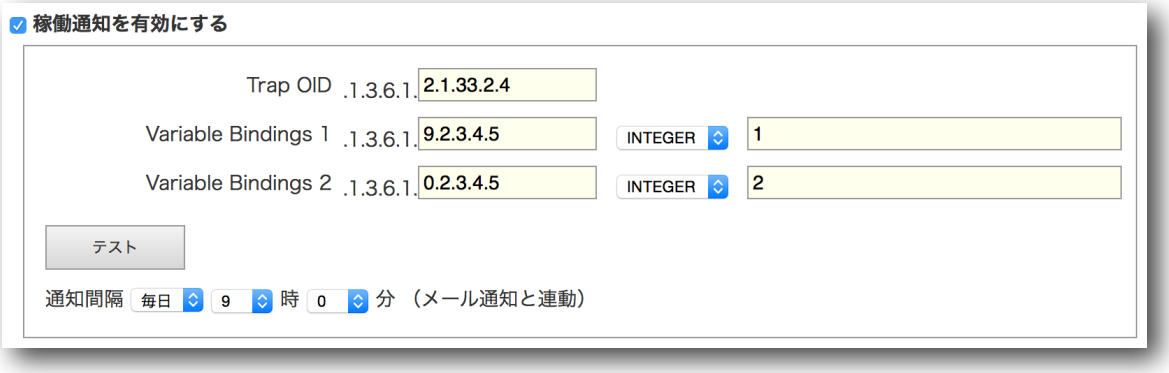
本製品が正常に稼働していることを定期的に通知します。

※Variable BindingsはIG2-03PL, IG2EX-03-08(24)VLのみの機能です。

(1) [稼働通知を有効にする] をチェックまたは解除することで、通知の 有効 / 無効 を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) 通知を有効にする場合には、あわせてOIDを設定します。また、稼働通知を送信する通知間隔を指定します。



3.7.12 イベント通知を有効にする

IntraGuardian2+が起動した場合等にSNMPトラップを送信します。

(1) [イベント通知を有効にする] をチェックまたは解除することで、通知の 有効 / 無効 を切り替えます。

TIPS:

稼働通知で指定する通知間隔は、メールの稼働通知の通知間隔指定と連動します。メールの稼働通知間隔とSNMPトラップの稼働通知間隔を別々に指定することはできません。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

＊ 各イベント発生時に送信されるSNMPトラップのOIDは表示の内容に固定されています。

TIPS:

[テスト]ボタンを押した場合、「IG2起動時」のSNMPトラップが送信されます。

3.7.13　SYSLOG通知

本製品のログをSYSLOGサーバへ通知するための設定を行ないます。

(1) [SYSLOG通知を有効にする] をチェックまたは解除することで、SYSLOG通知の 有効 / 無効 を切り替えます。

＊ 画面最下部の「確定」ボタンを押下したタイミングで反映されます。

(2) SYSLOG通知を有効にする場合には、あわせて下表の項目を設定します。

SYSLOGサーバ	SYSLOGサーバのIPアドレス
ログレベル	指定されたログレベル以上のログを通知する

TIPS:

本製品から発信される主なSYSLOGは以下の通りです。

INFOレベル:

[IGUARD] wget source address:...
[IGUARD] Signal received: ...
[WATCHDOG] ...
[DNS RESOLVER] set ipaddr:...
[DNS RESOLVER] change ipaddr:...
[DNS RESOLVER] set initial ipaddr:...
[SNIFFER] Many DNS resolve requests

NOTICEレベル:

Start iglaunch
Start IG-? ...
Stopping IG-? ...
End iglaunch
[IGUARD] START UP: version=...
[IGUARD] RESTART: version=...
[IGUARD] Initialize success
[IGUARD] terminate...
[IGUARD] SHUTDOWN: ...
"REGISTER: Illegal Host: lladdr=... inaddr=..."
"LOST: Illegal Host: lladdr=... inaddr=..."
No response from ..., restart network devices.
eth0 becomes up

WARNINGレベル:

[IGUARD] Connected to network
"DETECT: Illegal Host: lladdr=... inaddr=..."

ERRレベル:

[NOTIFIER] ...: error
[RESOLVER] software error.

なお、SYSLOGの内容は将来のバージョンアップで変更される事があります。

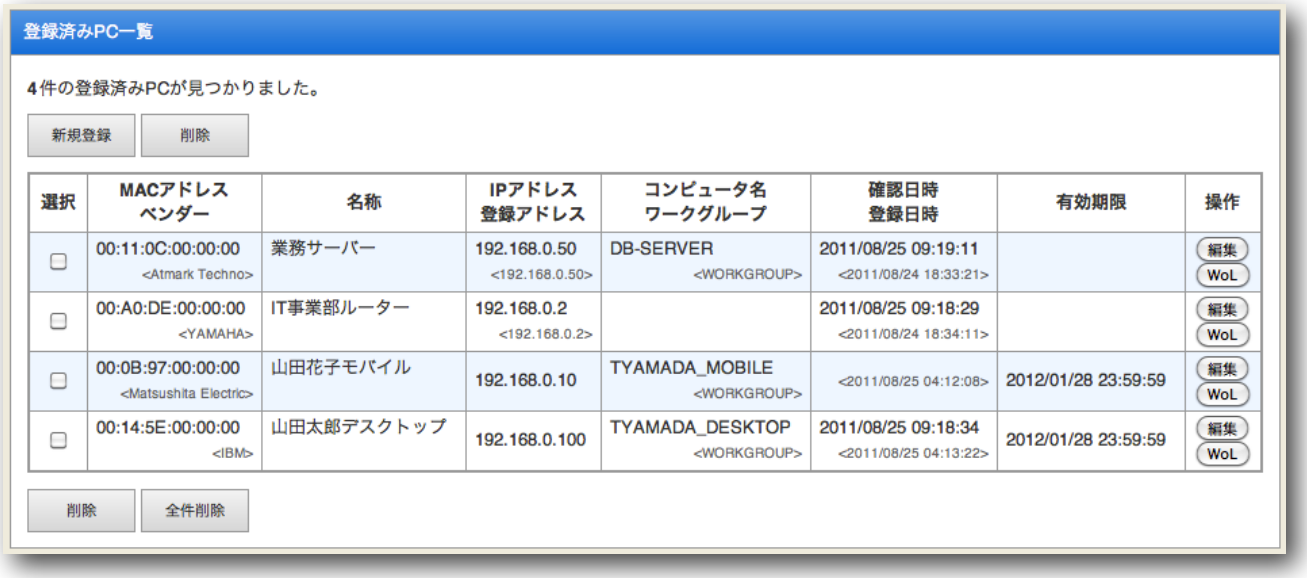
4　運用上の機能説明

ここからは、本製品を運用する際に必要となる機能について説明します。

4.1　登録済みPC一覧

本製品へ登録されているPCの一覧を表示します。

(1) メニューから「登録済みPC一覧」を押下します。
(2) 本製品に登録されているPCの一覧が表示されます。



4.1.1　新しいPCの登録

本製品へ新たにPCを登録します。

(1) 登録済みPC一覧画面の上部にある [新規登録] ボタンを押下します。
(2) 新規PC登録画面が表示されるので、下表の項目を入力します。

(3) [登録] ボタンを押下すると、登録ユーザーの情報が新しい内容へ変更されます。

名称	登録するPCの名称を入力します。 ,(カンマ)以外の任意の文字で、32バイト以内です。
MACアドレス	登録するPCのMACアドレスを入力します。
IPアドレス	登録する PC のIPアドレスを入力します。 登録時と異なるIPアドレスのPCを検出する機能を用いるときに参照されます。この機能を用いない場合（初期状態）は空欄で構いません。
有効期限	登録の有効期限を入力します。 YYYY/MM/DD HH:MM:SS の形式の文字列で指定します。 [カレンダー表示]　ボタンを押すと、右側にカレンダーが表示され、その日付をクリックすることにより本欄に入力を行うことができるようになります。

- 「動作設定」で [IPアドレス監視機能を有効にする] にチェックを入れている場合、ここで登録するIPアドレスと実際に検出されたIPアドレスが比較されることになります。登録IPアドレスが空欄であるPCは、IPアドレス監視の対象から外れます。
- 有効期限を過ぎた登録PCは、不正端末として扱われます。（検知/排除の対象となります。）
- 有効期限欄を空欄にすると、有効期限無しになります。

TIPS:

本製品を IntraGuardian2 Manager 等の管理ソフトウェアと組み合わせて運用し、データベース保存場所を「管理マネージャ」にしている場合、本製品の管理画面からPCの登録/編集/削除を行う事はできません。管理ソフトウェアより行なってください。

TIPS:

PCの登録は、最大40000件までできます。

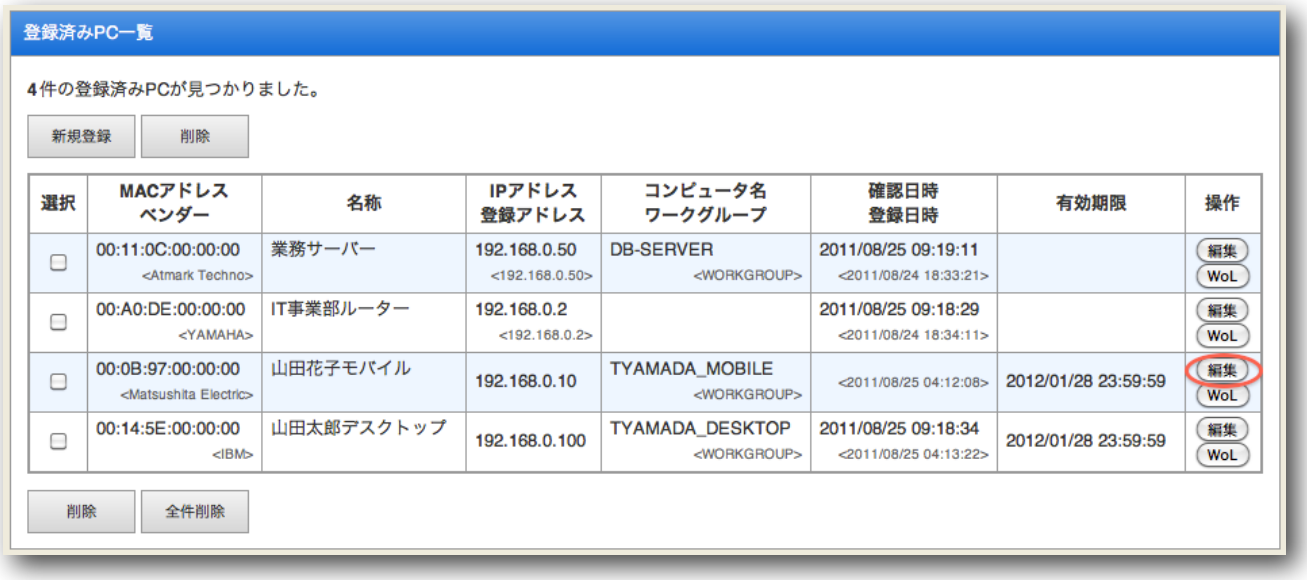
TIPS:

登録されたPCの情報は、本製品内のフラッシュメモリ上に保存されるので、本製品の電源を切っても消える事はありません。
ただし、本製品を IntraGuardian2 Manager と組み合わせて運用し、データベース保存場所を「管理マネージャ」にしている場合には、登録PCの情報は Manager が動作しているPCのハードディスク内に保存されます。本製品は電源投入時に Manager からこの情報を取り出し、動作を開始します。このため、本製品の電源投入時に何らかの理由で Manager と通信ができなかった場合には、本製品は不正PCの検知を行う事ができません。Managerと通信ができる状態にしてから、再度電源を入れ直してください。

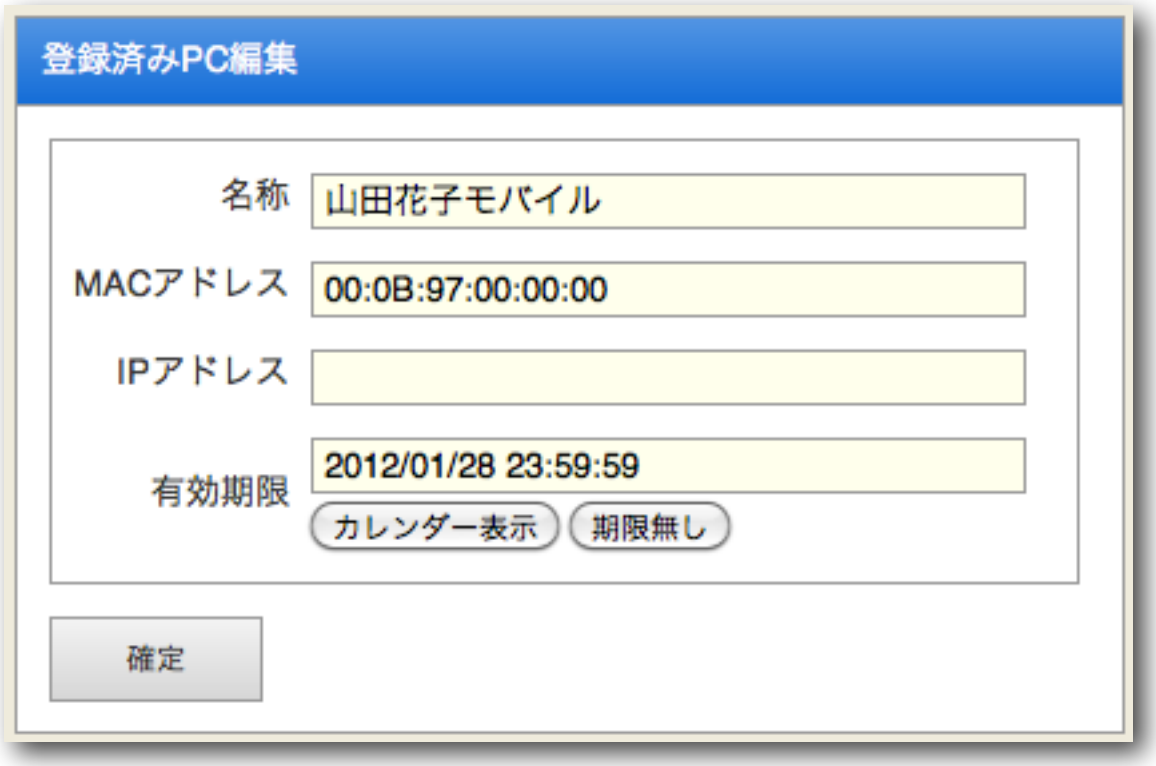
4.1.2　登録済みPCの編集

本製品へ登録されているPCの情報を編集します。

(1) 編集したいPC欄の右端にある［編集］ボタンを押下します。



(2) 登録済みPC編集画面へ遷移するので、変更する項目に新しい内容を入力します。



名称	登録するPCの名称を入力します。
MACアドレス	登録するPCのMACアドレスを入力します。
IPアドレス	登録する PC のIPアドレスを入力します。 登録時と異なるIPアドレスのPCを検出する機能を用いるときに参照されます。この機能を用いない場合（初期状態）は空欄で構いません。
有効期限	登録の有効期限を入力します。 YYYY/MM/DD HH:MM:SS の形式の文字列で指定します。 [カレンダー表示] ボタンを押すと、右側にカレンダーが表示され、その日付をクリックすることにより本欄に入力を行うことができるようになります。

(3) [確定] ボタンを押下すると、登録済みPCの情報が新しい内容へ変更されます。

TIPS:

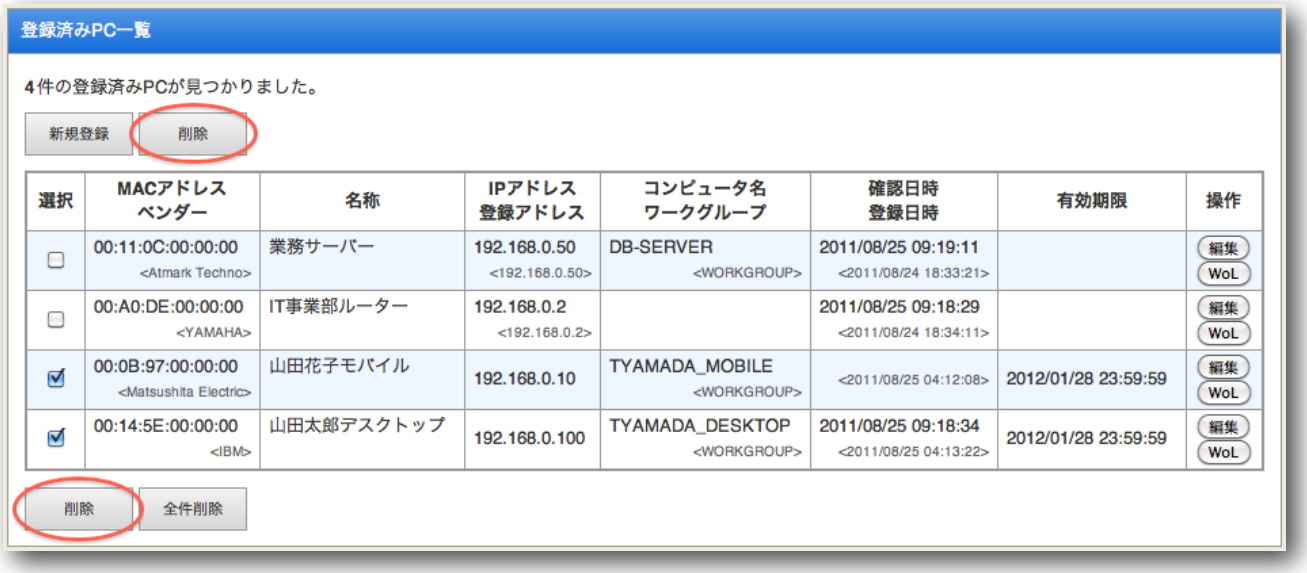
名称に入力できる文字数はおおよそ全角10文字です。半角では32文字入力可能です。

4.1.3　登録済みPCの削除

本製品へ登録されているPCを削除します。

(1) 削除したいPC欄の左端にあるチェックボックスをチェック状態にします。

＊ 複数のPCを削除する場合には、複数のチェックボックスをチェック状態にします。



(2) 表の左上または左下にある　[削除]　ボタンを押下すると、チェックしたPCが削除されます。

＊ 本製品の登録から削除されたPCは、削除後すぐに検知/排除の対象となります。

＊ どちらの [削除] ボタンを押しても動作に違いはありません。

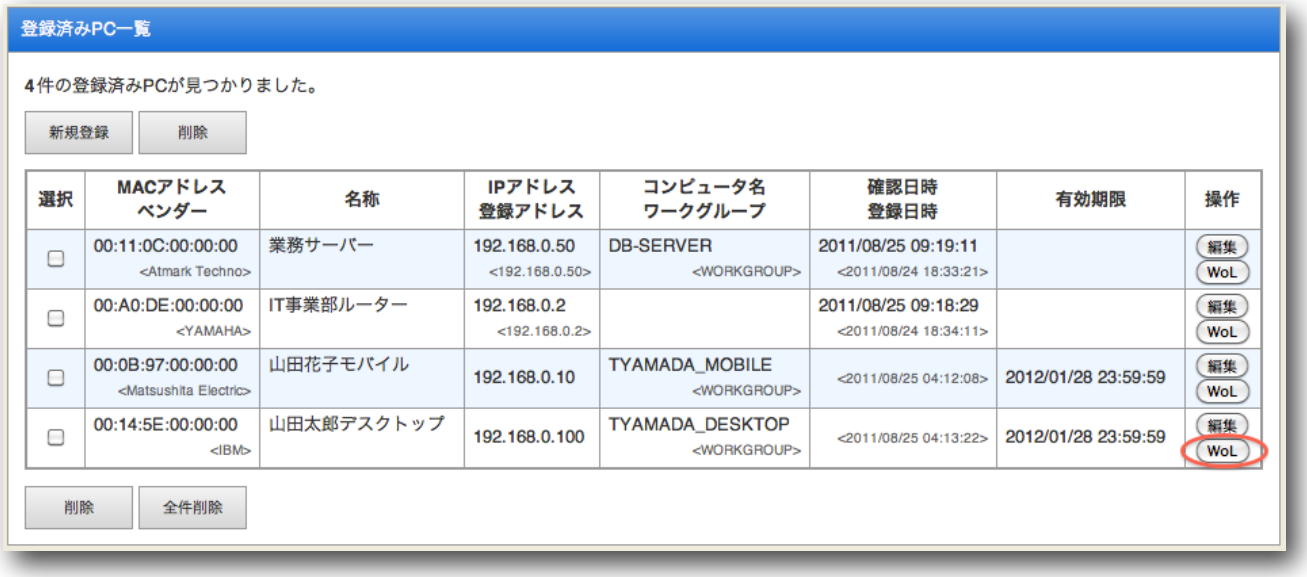
TIPS:

誤操作による事故を防ぐために、登録済みPCが1件も無い場合には、排除は行なわれません。

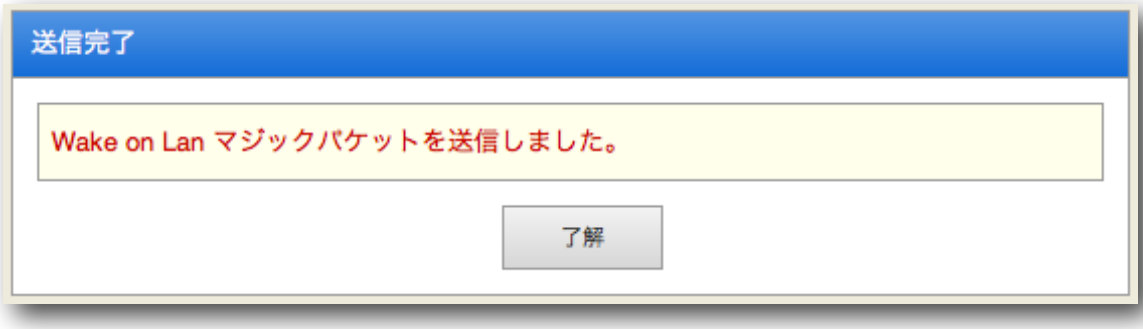
4.1.4　PCの起動

本製品へ登録されているPCを起動（電源ON）することができます。
ただし、本機能を使うためには、当該PCがマジックパケットによるWake　on　Lan機能（WoL機能）に対応している必要があります。

(1) 起動したいPC欄の右端にある［WoL］ボタンを押下します。



(2) 当該PCにマジックパケットを送信し、次の画面が表示されます。



＊ PCがWoL機能に対応しているかどうかはネットワークからは分かりませんので、本製品では全ての登録PCに対して [WoL] ボタンを表示しています。また、マジックパケットを送信した結果PCがきちんと起動したかどうかを確認することはできませんので、マジックパケット送信完了の表示のみを行なっています。

4.2　不正接続PC一覧

本製品が現在検知している不正接続PCの一覧を表示します。

(1) メニューから「不正接続PC一覧」を押下します。
(2) 不正接続PCの一覧が表示されます。

4.2.1　PCの登録

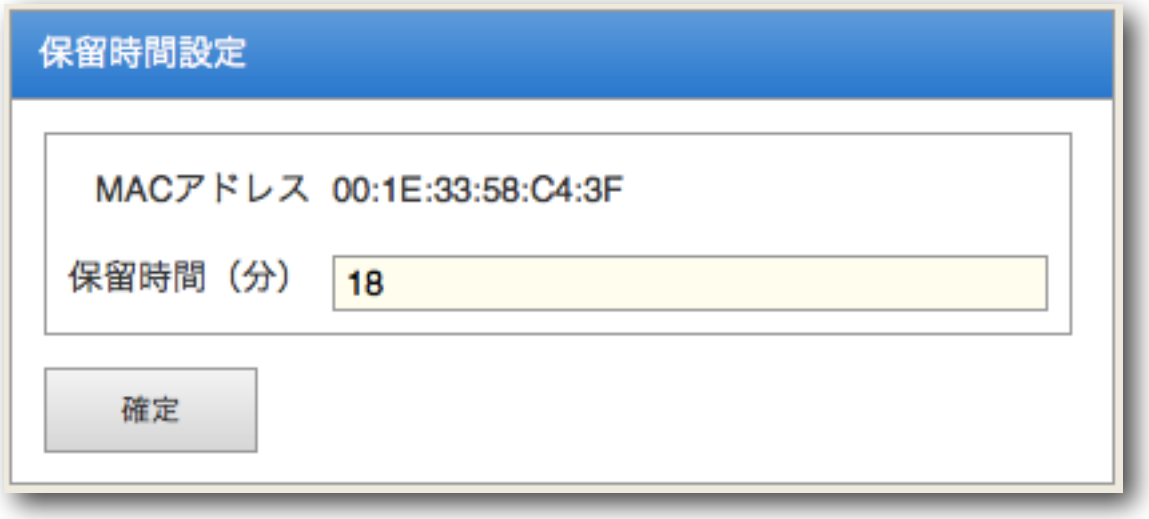
一覧に表示されているPCを、個別に本製品に登録します。

(1) 登録したいPC欄にある [登録] ボタンを押下します。
＊ 既に登録済みのPC欄には［登録］ボタンは表示されません。
(2) 新規PC登録画面へ遷移するので、【4.1.1　新しいPCの登録】と同様に、本製品へPCを登録します。

4.2.2　保留時間の変更

動作モードが「保留」になっているときは、一覧に表示されているPCの保留時間を変更できます。

(1) 操作欄の [保留] ボタンを押下します。
(2) 保留時間設定画面へ遷移するので、保留時間を分単位で入力し、[確定]　ボタンを押下します。



TIPS:

この画面で設定する保留時間は、このPCの残りの保留時間です。すなわち、「18」を設定すると、現在から18分後に保留状態が終わり、このPCは排除されます。
保留中のPCの保留時間を0にすると、すぐに排除が始まります。
逆に、排除中のPCの保留時間を1以上にすると、排除がいったん止まり、保留中の状態になります。

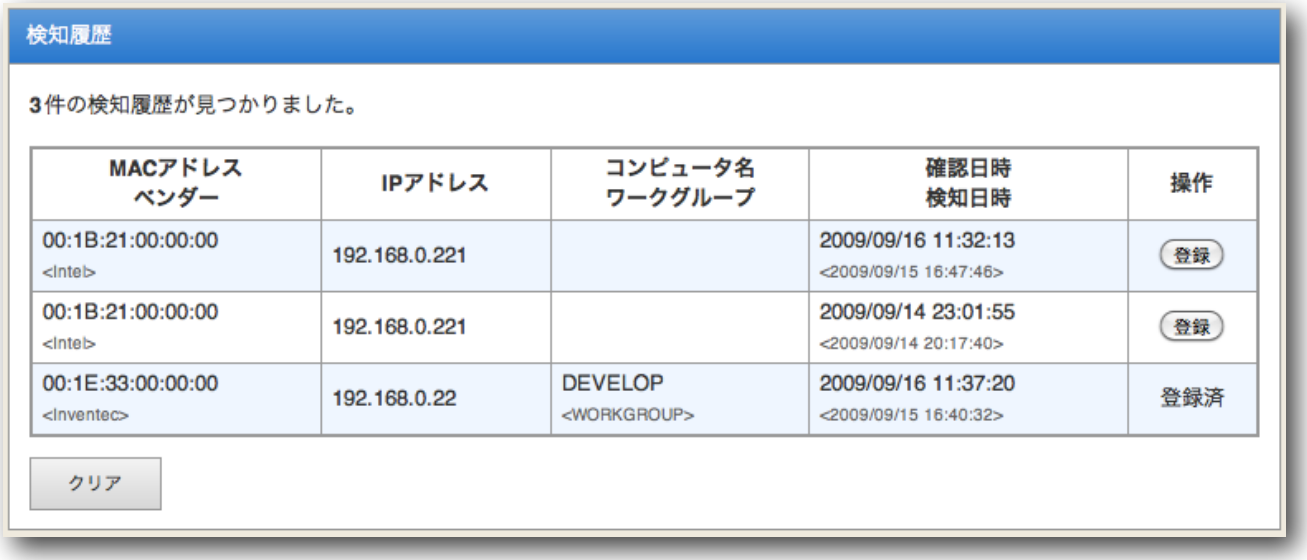
4.2.3 PCの一括登録

一覧に表示されているPCを全て本製品に登録します。

4.3　検知履歴

本製品が過去に検知した不正接続PCの一覧を表示します。

(1) メニューから「検知履歴」を押下します。
(2) 検知履歴の一覧が表示されます。



＊ 動作モードを保留に設定した場合、保留中の端末はネットワーク上からいなくなっても検知履歴に表示されませんのでご注意ください。

4.3.1　PCの登録

検知履歴に表示されているPCを、個別に本製品へ登録します。

(1) 登録したいPC欄にある［登録］ボタンを押下します。
＊ 既に登録済みのPC欄には［登録］ボタンは表示されません。
(2) 新規PC登録画面へ遷移するので、【4.1.1　新しいPCの登録】と同様に、本製品へPCを登録します。

4.3.2　検知履歴のクリア

検知履歴の内容をクリア（全て消去）します。
(1) 最下部にある [クリア] ボタンを押下すると、検知履歴がクリアされます。

TIPS:

検知履歴は本製品のRAM内に保存されているため、本製品の電源を切ると消えます。また、1000件を越えた場合、古い履歴から順番に消えます。
IntraGuardian2 Manager を用いると、検知履歴をManagerのハードディスク内に恒久的に保存する事ができます。詳しくはIntraGuardian2 Manager のスタートアップガイドをご覧下さい。

4.4　例外IPアドレス一覧

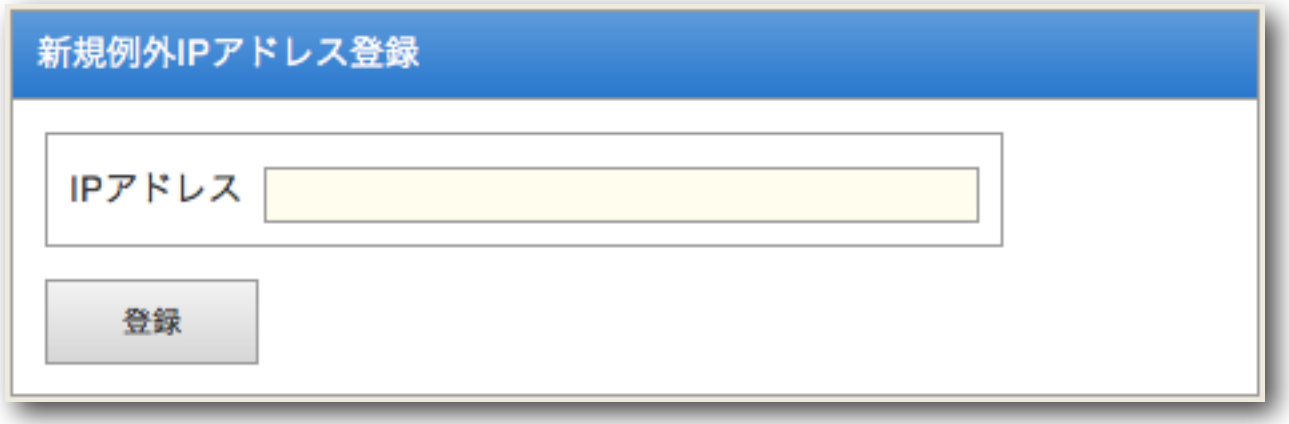
不正PCとして検知・排除する対象から除外する機器のIPアドレスの登録一覧を行ないます。

(1) メニューから「例外IPアドレス一覧」を押下します。
(2) 例外IPアドレスの一覧が表示されます。

4.4.1　例外IPアドレスの登録

例外IPアドレスを本製品に登録します。

(1) 例外IPアドレス一覧画面の上部にある [新規登録] ボタンを押下します。
(2) 新規例外IPアドレス登録画面が表示されるので、IPアドレスを入力し、[登録]　ボタンを押下します。



＊ 動作設定画面で「例外IPアドレスを有効にする」にチェックマークが付いていない場合、本画面で登録された内容は一切意味を持ちません。
＊ 例外IPアドレスの運用についての注意点は、【3.6.5 例外IPアドレス登録機能】をご覧下さい。

TIPS:
例外IPアドレスは最大で10件まで登録できます。

4.4.2 例外IPアドレスの削除

登録されている例外IPアドレスを削除します。

(1) 削除したいIPアドレスの左端にあるチェックボックスをチェック状態にします。
＊ 複数の登録を削除する場合には、複数のチェックボックスをチェック状態にします。

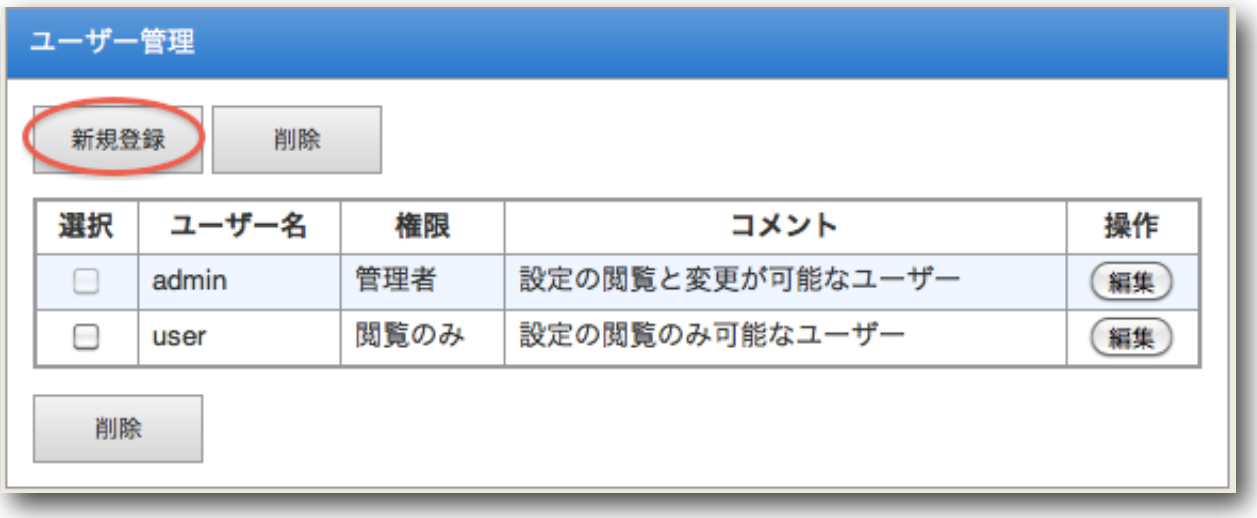
(2) 表の左上または左下にある [削除] ボタンを押下すると、チェックしたIPアドレスが削除されます。
＊ どちらの [削除] ボタンを押しても動作に違いはありません。

4.5　ユーザー管理

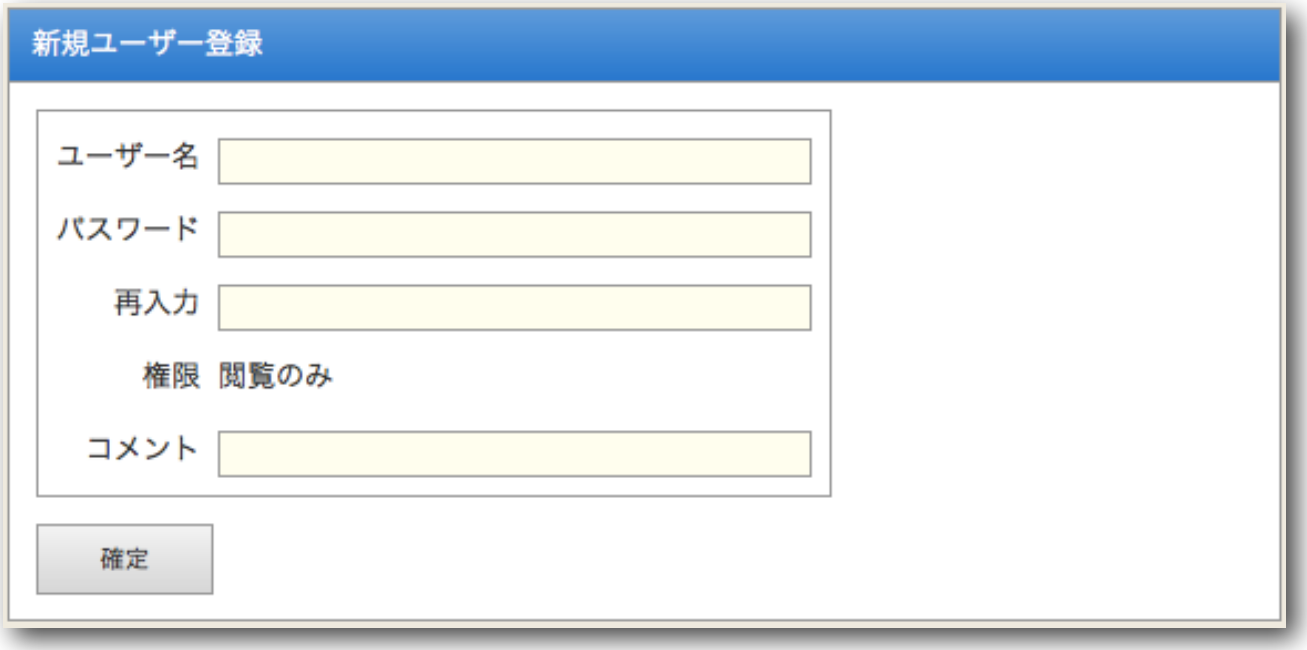
本製品の管理画面へログインするユーザーを管理します。

4.5.1　ユーザーの追加登録

(1) メニューから「ユーザー管理」を押下します。
(2) ユーザーの一覧が表示されます。一覧表の左上の [新規登録] ボタンをクリックします。



(3) 新規ユーザー登録画面が表示されるので、各項目に内容を入力します。
(4) [確定] ボタンを押下すると、新しいユーザーが増えます。



ユーザー名	4文字以上16文字以内の半角英数記号（‘,’(カンマ)を除く）を入力します。
パスワード	4文字以上16文字以内の半角英数記号（‘,’(カンマ)を除く）を入力します
再入力	上記のパスワードを再入力します
コメント	このユーザーの説明文を入力します。32文字以内の任意の文字が使用できます。（‘,’(カンマ)を除く）

TIPS:

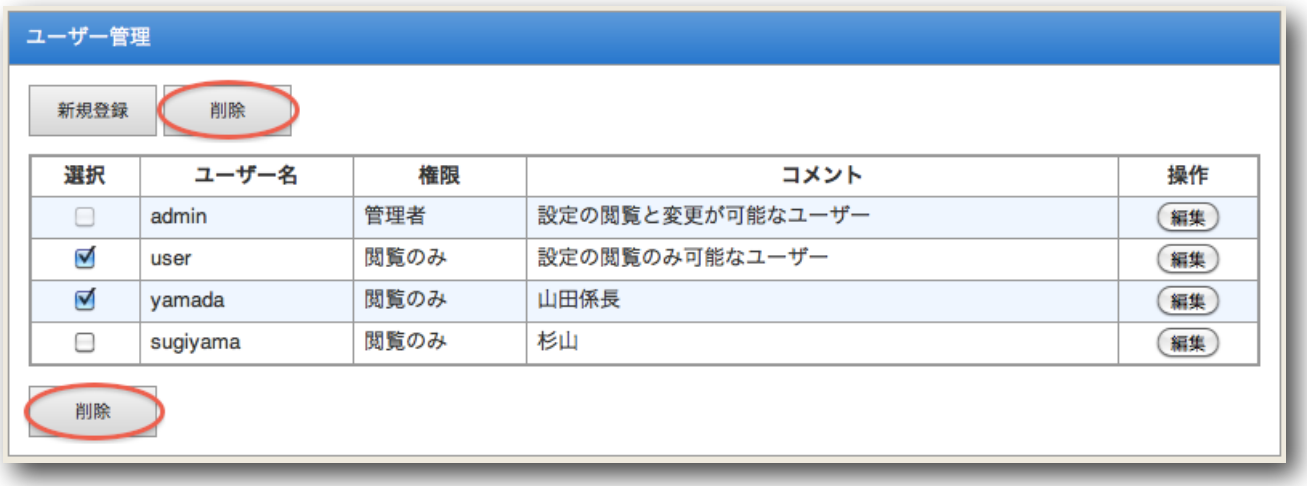
ユーザーは最大で5名まで登録できます。

4.5.2　ユーザーの編集

ユーザーの一覧表にある [編集] ボタンを押下すると、そのユーザーの情報を変更することができます。
パスワードを変更しない場合には、パスワード欄と再入力欄をともに空欄にした状態で、[確定] を押下してください。

4.5.3　ユーザーの削除

ユーザーの一覧表のチェックボックスにチェックを入れて [削除] ボタンを押下すると、選択したユーザーを削除することができます。



＊ 上の [削除] ボタンを押しても下の [削除] ボタンを押しても、動作は同じです。

4.6　ファームウェア更新

本製品に組み込まれている不正接続検知／排除システムソフトウェア（『ファームウェア』という）を更新します。
本製品のファームウェアは、製品サポートサイトにて配布される更新ファームウェアにより更新できます。

(1) メニューの「再起動」を押下します。
(2) 「再起動ボタンを押下すると、IntraGuardian2　を再起動します」というメッセージが出ますので、[再起動] ボタンを押下します。
(3) 1分程度待って本体の赤LEDが消えているのを確認し、再度管理画面にログインします。

(4) メニューから「ファームウェア更新」を押下します。
(5) [ファイルを選択] ボタンをクリックし、あらかじめ製品サポートサイトからダウンロードしておいた、本製品の更新ファームウェアを選択します。
(6) [実行] ボタンを押下します。

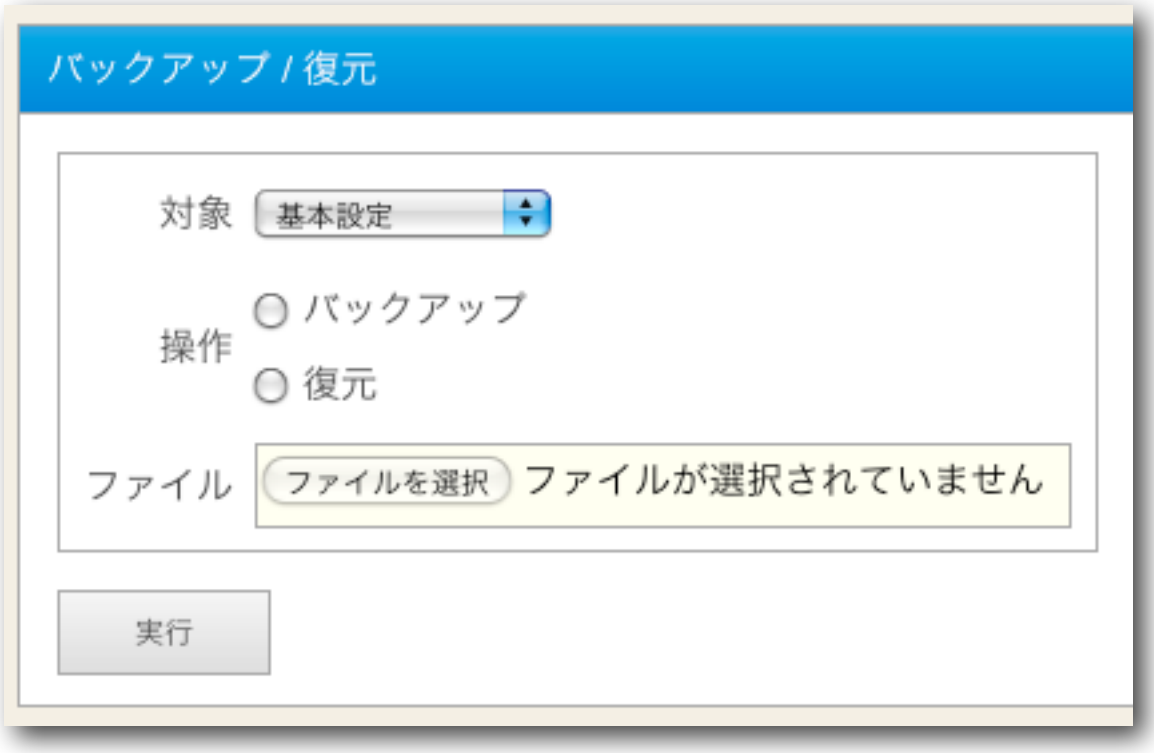
(7) ファームウェアの更新が開始され、約２～4分後に自動的に再起動します。

＊ ファームウェアの更新中は　ステータスLED3が赤点滅します。また、更新が完了して再起動をしている間はステータスLED1が赤点滅状態になります。
＊ ファームウェア更新中は絶対に電源を抜かないようご注意下さい。万が一、更新中に電源が抜かれた場合本製品が起動しなくなる恐れがあります。

4.7　バックアップ / 復元

本製品の基本設定や登録済みPC一覧、例外IPアドレス一覧をバックアップ / 復元します。

(1) メニューから「設定ファイル」を押下します。
(2) 操作の対象（[基本設定] [登録済みPC一覧] または [例外IPアドレス一覧]）をリストから選択します。
(3) 実行したい内容にあわせて操作（[バックアップ] または [復元]）を選択します。
(4) 復元を実行する場合には [ファイルを選択] ボタンをクリックし、あらかじめバックアップしておいたファイルを選択します。
(5) [実行] ボタンを押下すると、バックアップ / 復元を実行します。
(6) 操作にて [バックアップ] を選択した場合、バックアップファイルのダウンロードが開始され、[復元] を選択した場合、バックアップファイルから復元が開始されます。



＊ 設定を復元して本製品のIPアドレスが変わった場合、ブラウザで新しいIPアドレスにアクセスしてログインしなおしてください。

TIPS:

登録済みPC一覧をバックアップすると、”hostdb.csv”という名前のファイルがダウンロードされます。このファイルはCSV形式の単純なテキストファイルで、これを適当なテキストエディタで編集し、「復元」操作で復元する事により、多数のPCの登録を一気に行う事ができます。
“hostdb.csv”ファイルのフォーマットは、次のようになっています。

1行目: フォーマットバージョン番号（“2.2.0”）
2行目: 項目内容のコメント
3行目以降: 登録PC情報

登録PC情報の各カラムは、次のようになっています。

MACアドレス, IPアドレス, 名称, 登録日時, 有効期限, 登録ネットワークアドレス, PC移動監視除外フラグ, ホスト名変更監視除外フラグ

MACアドレス以外の項目は空欄でも構いません。
名称に日本語を用いるときにはShift-JISコードを使ってください。文字数は全角文字で10文字以下にしてください。
有効期限を設定しない場合には、空欄にしてください。
登録ネットワークアドレスは、登録時に所属していたネットワークアドレスです。不明の場合は空欄で構いません。
PC移動監視除外フラグは0または1の数字で、IntraGuardian2 ManagerのPC移動履歴機能が用いる情報です。不明の場合は空欄で構いません。
ホスト名変更監視除外フラグは、現バージョンのソフトウェアでは使用していませんが、必ず0にしておいて下さい。

“hostdb.csv”ファイルの例:

```
2.2.0
00:0D:02:00:00:00,192.168.0.1,ルータ,2009/09/11 17:48:03,2010/09/10 23:59:59,192.168.0.0,0,0
00:14:5E:00:00:00,192.168.0.100,山田太郎デスクトップ,2009/09/11 17:48:03,,192.168.0.0,0,0
00:0B:97:00:00:00,192.168.0.10,山田モバイル,2009/09/11 17:48:03,2010/01/01 00:00:00,192.160.0.0,0,0
00:11:0C:00:00:00,192.168.0.50,業務サーバ,2009/09/11 17:48:03,,192.168.0.0,1,0
```

- 空欄の項目の部分を”,,”（カンマ2つ）にする事と、”.”（ピリオド）と”,”（カンマ）の違いに注意してください。
- “#”で始まる行と空行は読み飛ばされます。なお、改行コードはCR+LFを使ってください。
- このファイルフォーマットは2.0.14で変更されました。IntraGuardian2+ は、以前のフォーマットで書かれたファイルも読み取ることができます。

4.8　再起動

管理画面から本製品を再起動します。

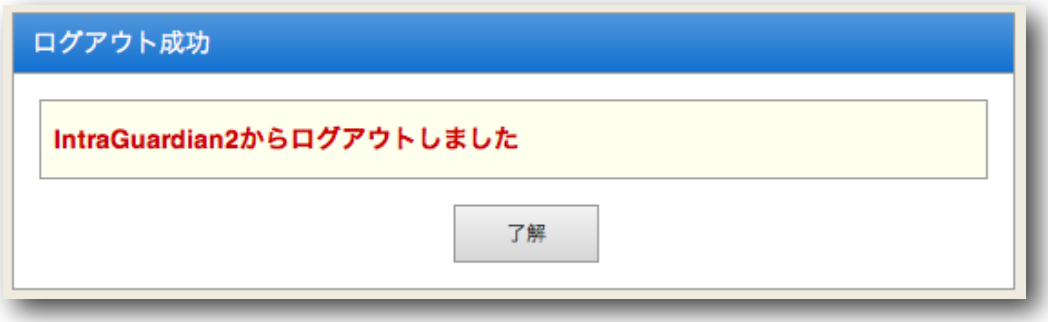
(1) メニューから「再起動」を押下します。
(2) [再起動] ボタンを押下します。
(3) 自動的に本製品が再起動されます。

＊ 再起動中は本製品のステータスLED1とステータスLED3が赤点滅します。再起動が終了するとステータスLED1が緑点滅に変わりますので、あらためてブラウザで本製品の管理画面にアクセスしてください。

4.9　ログアウト

本製品の管理画面からログアウトします。

(1) メニューから「ログアウト」を押下します。
(2) ログアウトすると、以下の画面が表示されます。



(3) [了解] ボタンを押下すると、ログイン画面へと遷移します。

IntraGuardian2+
スタートアップガイド
Version 2.5
2015年9月14日

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/