不正接続検知／排除システム

IntraGuardian2+
IntraGuardian2+EX

（Version 3.6.0 ～）

スタートアップガイド

第11版

2020年05月22日

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⁺(以下「本製品」)をお買い上げいただき、誠にありがとうございます。

本ガイドは、以下の製品についてご利用方法を解説しています。

名称	製品型番
IntraGuardian2⁺	IG2-03PL
IntraGuardian2⁺ EX 8セグメント対応版	IG2EX-03-08VL
IntraGuardian2⁺ EX 24セグメント対応版	IG2EX-03-24VL

本製品を利用する前に、本ガイドをよく読んで正しくお使いください。

ご注意

- 本ガイド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。
- 本ガイドの内容は、将来予告なく変更することがあります。

本製品に関する最新の情報は、製品サポートサイト

https://intraguardian.jp/

をご覧ください。

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

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

目次

安全上のご注意

ご使用の前に、安全上のご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・解析は禁止されています。
- 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います。
- 本製品のハードウェアの転用は禁止されています。
- 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。

VCCI-A対応

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。その場合、使用者が適切な対策を講ずるよう要求されることあります。

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。

利用許諾契約

日本シー・エー・ディー株式会社及びそのライセンサー(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」上のソフトウェア及び同製品用集中管理ソフトウェアである「IntraGuardian2+ Manager Professional」(以下併せて「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、お客様が本契約のすべ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、本ソフトウェア関連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に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　利用許諾
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。IntraGuardian上のソフトウェアに関しては、IntraGuardian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類似製品・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　サポート
1. 本ソフトウェアの更新等のサービスは、別途締結されるサポート契約のもとで提供いたします。

第6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7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8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9条　権利行使
お客様は、NCAD(そのライセンサーを含む)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10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。

最新更新日:2018年4月24日
日本シー・エー・ディー株式会社
ネットチャート株式会社

1 製品概要

1.1 本製品(IntraGuardian™シリーズ)について

本製品「IntraGuardian」は企業内などのイントラネットワークへ接続されているPC(パソコンの他、スマートホンやネットワーク機能付のゲーム機などを含みます)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大きな効果を期待できます。**IntraGuardian単体で通知できるメールアドレスは1つです。複数のメールアドレス宛にメール通知したい場合は集中管理ソフトウェア「IntraGuardian2⁺ Manager Professional」をご利用ください。

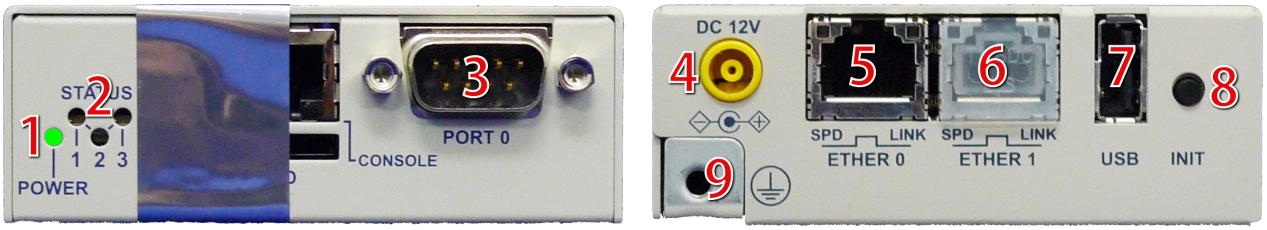
1.2.3 不正接続PC排除

本製品の不正接続PC排除機能を有効にしておくことで、管理者が不在の場合でも管理者自身に代わり、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。

2 ご使用の前に

本製品をご使用いただく前に必要な、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
3	シリアル端子(メンテナンス用につき、使用しないでください)
4	電源端子
5	LAN端子
6	拡張LAN端子(将来の拡張用につき、使用しないでください)
7	USB端子(メンテナンス用につき、使用しないでください)
8	初期化ボタン
9	アース端子

✴ 3、6、7はメンテナンスや修理のために、指定された技術者のみが使用する端子です。お客様がこれらの端子を使用することで機器の不具合が起きた場合、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のでご注意ください。

注意！
ステータスLED横の封印シールを剥がすと保守サポートの一切を受けられなくなりますので、絶対に剥がさないでください。

2.2 準備するもの

機器本体	本製品です。
ACアダプタ	本製品に同梱されています。
アース線	アースを設置する場合、専用ケーブルを別途ご用意ください。
LANケーブル （ストレート）	長さ約1mのLANケーブルが1本、同梱されています。
管理用PC	お客様ご自身でご用意ください(※推奨スペックについては下記＊を参照ください)。

＊ 管理用PCのスペックに関しては、イーサネットのLANポートを有し(無線LANは不可)、かつ一般的なWebブラウザさえ動作させることができればIntraGuardianの運用が可能です。IntraGuardianを運用するにあたり、管理用PCに本製品専用の特別なソフトウェア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AC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

本製品は、接続されているACアダプタの電源ケーブルを抜くと動作を終了します。なお、設定情報の書き込みを行なっている最中に終了してしまうと設定情報が正しく保存されない事がありますので、LEDが1個でも赤く「点灯」している時は電源ケーブルを抜かないでください。

2.5 リセット

初期化ボタンを5秒以上押すと、本製品はリセットされます。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います。ステータスLED1が緑点滅になるまで約2分かかります。

初期化(INIT)を約5秒間押し続ける

ステータスLED3が一瞬光る

初期化(INIT)を離す

✴ 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き、再度差してください。

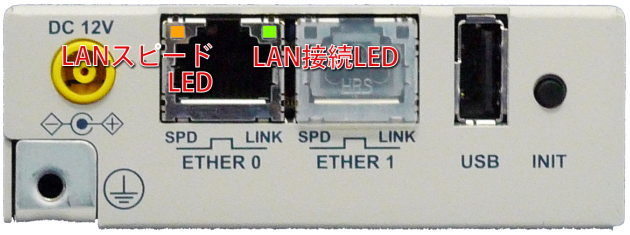
3 ネットワーク接続の設定

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。



起動後、本製品が正常に動作している時、各LEDは次のようになります。

電源LED(POWER)	緑点灯
ステータスLED1	緑点滅(2回ずつ点滅) 起動途中は赤点滅します。
ステータスLED2	消灯
ステータスLED3	消灯 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LED(SPD)	点灯 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)	不定期に点滅 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。

本製品のイーサネットポートは 10Mbps・100Mbps および 1000Mbps に対応しています。通信速度およびLANケーブルのストレート／クロスは自動認識します。

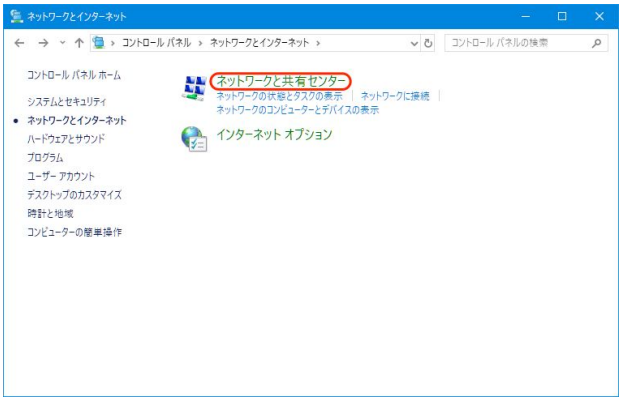
3.2 本製品の管理画面にアクセス

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。

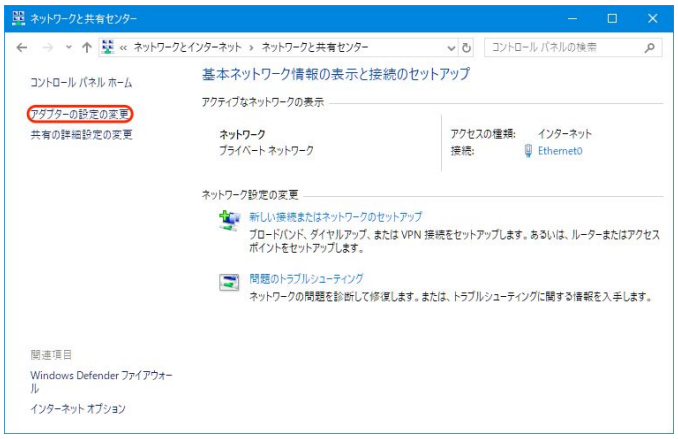
3.2.1 管理用PCのネットワーク準備(Windows10)

本製品の初期設定を行うためには、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、Windows10のPCのネットワーク設定について説明します。macOSを使用する場合は次項を参照してください。その他のOSを使用する場合は、そのOSの説明書などを参照し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、本項と異なる画面が表示されることがあります。

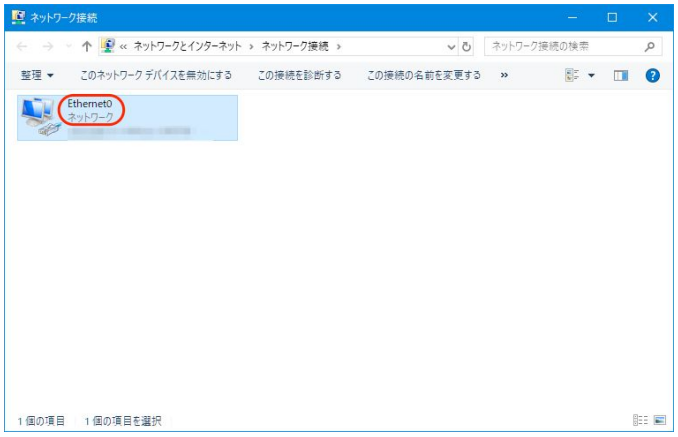
コントロールパネルから「ネットワークとインターネット」を開きます。



[ネットワークと共有センター]をクリックします。

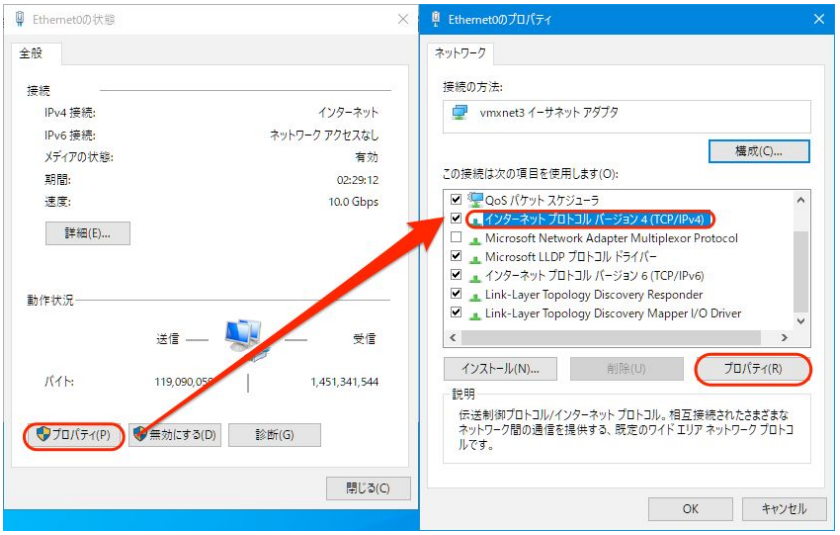


[アダプターの設定の変更]をクリックします。



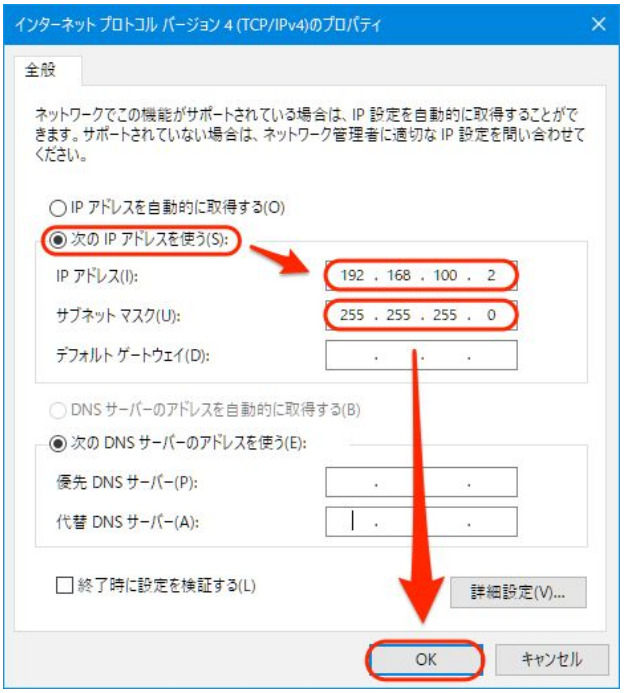
IntraGuardian2+が接続されているネットワークアダプタをダブルクリックします。

[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)」を選択して[プロパティ]をクリックします。

「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。

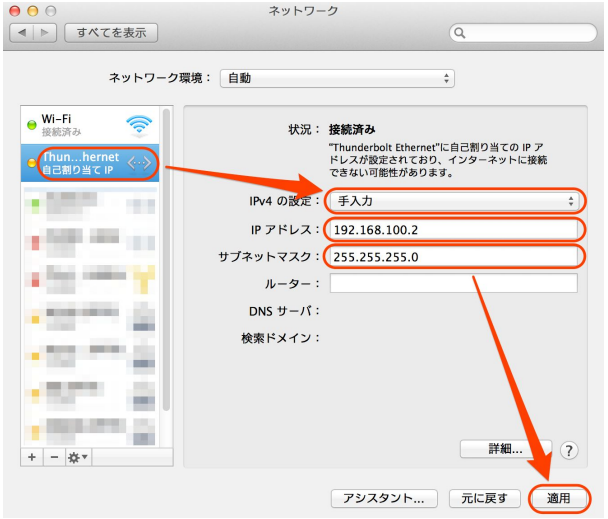


これで、管理用PCのネットワーク準備は完了です。

3.2.2 管理用PCのネットワーク準備(macOS)

本項では、macOSのネットワーク設定について説明します。ハードウェア構成によっては、本項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は、使用するブラウザ、ファームウェアのバージョン等により実際の表示と異なる場合があります。

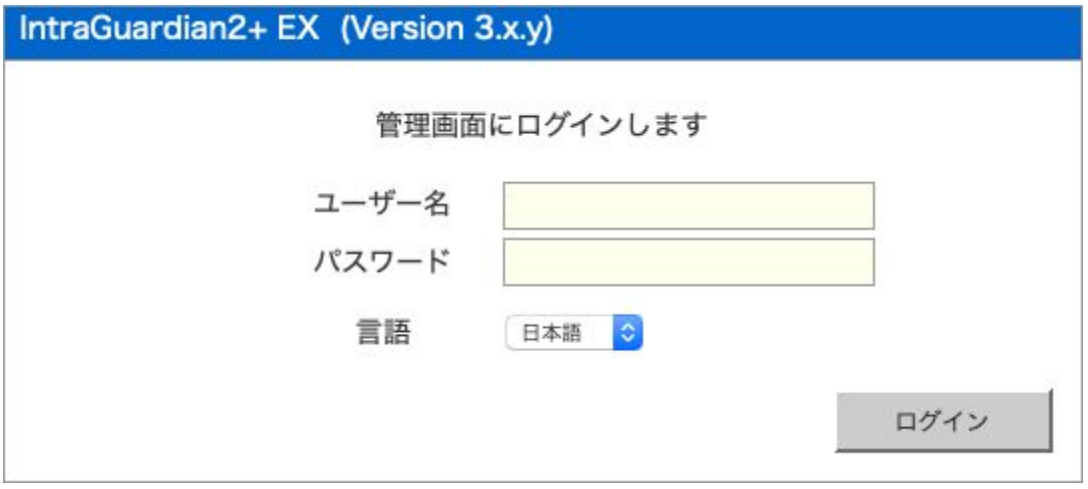
3.2.4 本製品の初期IPアドレスを入力

本製品は、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IP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。

＊ 製品名やバージョンはお買い求めいただいた製品や、次期によって若干異なります。



「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、出荷時は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、利用中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、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 本体管理メニュー

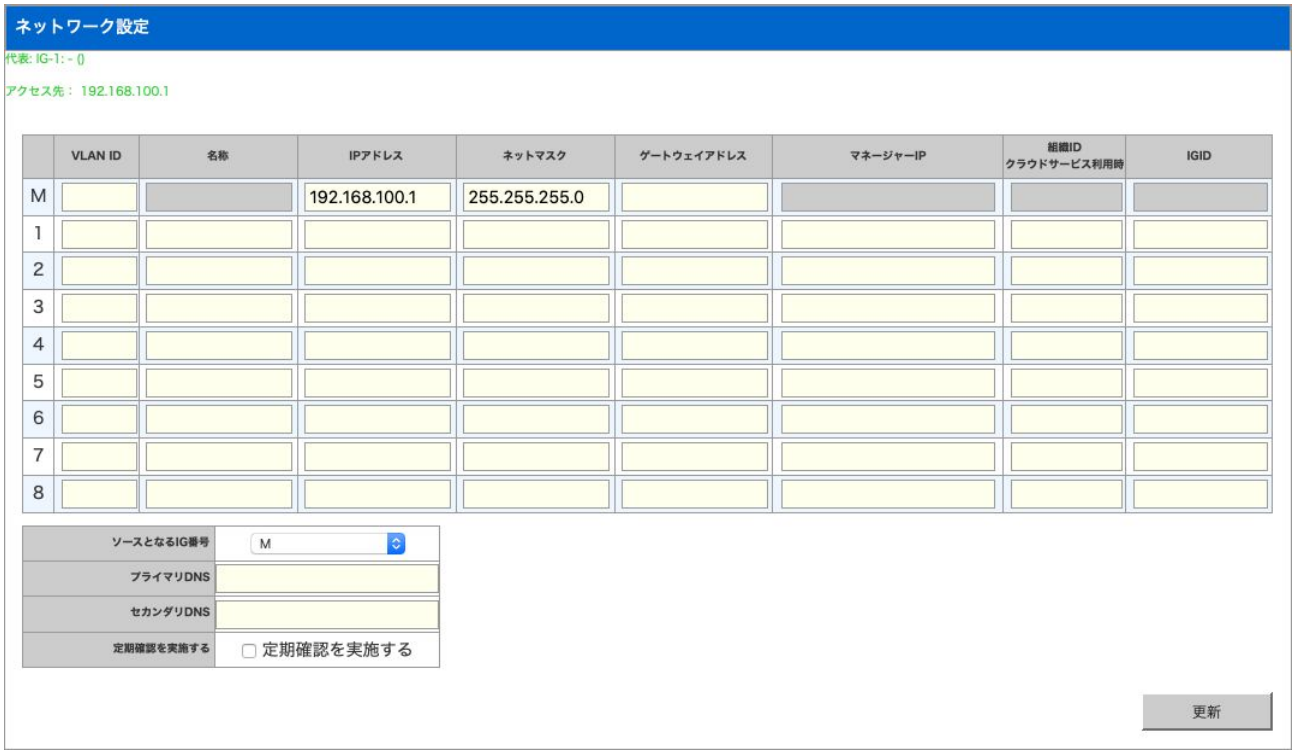
ログイン後に表示される管理画面の右上に、以下のメニューが表示されます。最初に、このメニューから[ネットワーク]を選んでネットワークの設定を行います。

＊ 画面はIntraGuardian2+ EXのものです。

3.4 ネットワーク設定

メニューの[ネットワーク]をクリックし、左側に表示される[ネットワーク設定]をクリックすると次の画面が開きます。

IntraGuardian2+ EX



IntraGuardian2+ EXには8VLAN製品と24VLAN製品があります。ネットワーク設定画面には最初からセグメント枠が用意され、数字が割り振られている行がそれに当たります。Mが割り振られている行は、この管理画面へのアクセスに限定されたネットワークです。初期設定ではIntraGuardian2+EXのイーサネットポートは「Untagged」、IPアドレスは「192.168.100.1」です。

TIPS:
M行のネットワークでは監視や排除機能は動作しません。

IntraGuardian2+

項目説明

VLAN ID (IG2EX-03-08VL、IG2EX-03-24VLのみ)	ネットワークのVLAN ID ✶ 1から4094までの範囲で入力してください。 ✶ UntaggedはVLAN IDを空白とし、一行のみ設定可能です。
名称	本機器の名称を設定することができます。設定した名称は、ログイン画面やメール通知に表示されるようになります。 ✶ IntraGuardian2+ Manager Professional連携時はセクション名になります。
IPアドレス	本機の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
ゲートウェイアドレス	設置するネットワークのゲートウェイのIPアドレス
マネージャーIP	IntraGuardian2+ Manager Professionalのアドレス アドレスはカンマ区切りで3つ入力可能です。 ✶ IntraGuardian2+ Manager Professional Ver.3系のみ利用可能で、それ以前のバージョンでは利用できません。
組織ID (クラウドサービス利用時のみ)	事業者に指定されたID
IGID	IntraGuardian2+ Manager Professional利用時 自動採番されたIDが表示されます。
ソースとなるIG番号 (IG2EX-03-08VL、IG2EX-03-24VLのみ)	SNMP・SMTP・NTPを使用するとき、指定したVLANのIPアドレスがソースIPとなります。
プライマリDNS セカンダリDNS	DNSサーバーのIPアドレス
定期確認を実施する	ソースとなるIGのデフォルトゲートウェイへの定期的なPING要求により通信チェックをする場合、チェックマークを付けます。

[更新]ボタンをクリックすると、新しいインターフェース設定で動作します。

✴ 設定を確定した直後は、内部でネットワーク構成の再構築などの調整作業が行なわれているため、各ページへのアクセスが一時的にできなくなる場合やエラーが表示される場合があります。20秒～数分待ってから次の操作を行なってください。

TIPS:

「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、ソースとなるIGのデフォルトゲートウェイで指定される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、本製品のネットワークインターフェースを初期化し直します。この機能は、本製品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。デフォルトゲートウェイがない場合は定期確認は実施されませんのでご注意ください。

3.5 システム設定

メニューの[システム]欄にある[システム時刻] 、[IGID・ステータス]、[パケットキャプチャ]、[バックアップ]、[ファーム]、[ログ]、[初期化]、[再起動]の各項目は、本製品の運用時に使用します。

3.5.1 システム時刻

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。[パソコンの時刻に合わせる]にチェクを入れると、本製品搭載のリアルタイムクロックをアクセスしているパソコンの時計に合わせることができますが、月に数分程度の誤差が生じる場合があります。正確な時刻情報を得るためにはタイムサーバの指定を行います。

項目説明

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IPアドレスかドメイン名を入力します。 ＊ 時刻同期は本設置設定を確定した直後、起動時、および起動後30分毎に行ないます。
パソコンの時刻に合わせる	この項目をチェックすると、パソコンの時刻に手動であわせることができます。NTPサーバが利用できない環境に設置する際に使用します。
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をご覧ください。
http://jjy.nict.go.jp/tsp/PubNtp/index.html

3.5.2 IGID・ステータス

IntraGuardian2+ Manager Professional との接続状況が表示されます。設定を行ったにもかかわらず接続状態が「OK」にならないときは、改めて設定をご確認ください。

IGID・ステータス

VLAN ID	接続中のマネージャ	接続状態	送信	受信	IGID
1		OK	378.5バイト	8.9バイト	
2		OK	205.3バイト	8.9バイト	
3		OK	155.8バイト	8.9バイト	
4		OK	106.3バイト	8.9バイト	
5		OK	131.1バイト	8.9バイト	
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					

TIPS:

IG識別IDは、管理マネージャVer3系を利用した際の内部管理番号です。本画面ではIG識別IDを変更することはできません。

TIPS:
接続中マネージャの状態表示は、「管理マネージャ Ver.3 系」を選択した場合に表示されます。

3.5.3 パケットキャプチャ

何らかのトラブルが発生した際、サポート窓口よりパケットキャプチャを依頼することがあります。その場合はこの画面でパケットキャプチャを行った結果をダウンロードすることができます。なお、キャプチャファイルは、独自暗号されておりサポート窓口以外見ることはできませんのでご注意ください。

＊「対象」はIntraGuardian2+ EXでのみ選択できます。

3.5.4 バックアップ

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) 操作の対象([基本設定]、[登録済みPC一覧]、[例外IPアドレス一覧])をリストから選択します。
(2) 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。
(3) 復元を実行する場合、[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。
(4) [実行]ボタンをクリックすると、バックアップ/復元を実行します。
(5) 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。
- Version 3.0 から例外IPアドレスも登録済みPC一覧へ含まれるようになりましたが、過去のバージョンで取得したデータの復元は可能です。
- 基本設定(装置全体)はIntraGuardian2+ EXのみでご利用可能です。
  この中にはVLAN設定も含まれます。

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、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。

3.5.5 ファーム

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(ファームウェアと呼びます)を更新します。

本製品のファームウェアは、公式サイトの製品サポートで配布される更新ファームウェアより更新できます。なお、本製品用のファームウェアは、

IntraGuardian2⁺用
"IntraGuardian_MAE320_Firmware.x.x.x.bin"

IntraGuardian2⁺ EX 8VLAN用
"IntraGuardian_MAE320UM_Firmware.x.x.x.bin"

IntraGuardian2⁺ EX 24VLAN用
"IntraGuardian_MAE320VM_Firmware.x.x.x.bin"

というファイル名です。必ず、お買い求めになった製品に適合したファームウェアを使用してください。

(1) メニューの[再起動]をクリックします。
(2) 「再起動ボタンをクリックすると、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]ボタンをクリックします。
(3) 約2分経過後に本体の赤LEDが消えているのを確認し、管理画面に再ログインします。
(4) メニューから[ファームウェア更新]をクリックします。
(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。
　✶ 詳細は製品サポートサイト http://intraguardian.jp をご覧ください。
(6) [実行]ボタンをクリックします。

(7) ファームウェアの更新が開始され、約2～4分後、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、更新完了後に再起動中はステータス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ください。万が一、更新中に電源を抜いた場合、本製品が起動しなくなる恐れがあります。

3.5.6 ログ

本製品のログをSYSLOGサーバへ通知するための設定を行います。

(1) [SYSLOGを有効にする]を有効または無効にすることで切り替えます。

✶ 画面右側の[更新]ボタンをクリックしたタイミングで反映されます。

(2) SYSLOG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。

項目説明

SYSLOGサーバ	SYSLOGサーバのIPアドレス ✶ FacilityはUSER2固定です。
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

また画面下部には、本装置に保存されたログが表示されています。必要に応じてダウンロードすることも可能です。

3.5.7 初期化

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います。

＊ 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き、再度差してください。

この操作では、全ての設定が初期化されてしまいます。一部の設定のみを初期化したい場合はこの画面をご利用ください。

初期化するためには、毎回ランダム生成される初期化パスワードを初期化パスワード入力欄に入力する必要があります。

3.5.8 再起動

(1) メニューから[再起動]をクリックします。
(2) [再起動]ボタンをクリックします。
(3) 自動的に再起動します。

✶ 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、改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 ネットワーク監視機能設定

ここからはIG2本体(**IntraGuardian2+ Manager Professionalを利用しない場合**)の設定になります。

IntraGuardian2+では起動時からネットワーク監視プログラムが動作していますが、IntraGuardian2+ EXでは、【3.4　ネットワーク設定】の操作を終えると、本製品の内部で設定したVLANネットワークセグメントの数と同じ個数のIntraGuardian2+ネットワーク監視プログラムが並列に稼働し始めます。これらのプログラムは原則としてそれぞれ独立に動作し、IntraGuardian2+を複数台設置したものと同等に取り扱うことができます。

4.1 ログイン

本装置の設定したIPアドレスにウェブブラウザからアクセスすると、ログイン画面が表示されます。ログイン画面や出荷時のユーザー名・パスワードは【3.2.4　ネットワーク設定】、英語での利用については【3.2.5 英語での利用】をご覧ください。

4.2 メニュー項目

管理画面の左側は、右上のメニューで選択したボタンに応じて、以下のサブメニューが表示されます。

TOP

システム

ネットワーク

アカウント

4.3 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[不正接続一覧]をクリックします。
(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]ボタンをクリックします。全件一括で登録する場合には、画面最下部の[全件登録]ボタンをクリックします。
(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。

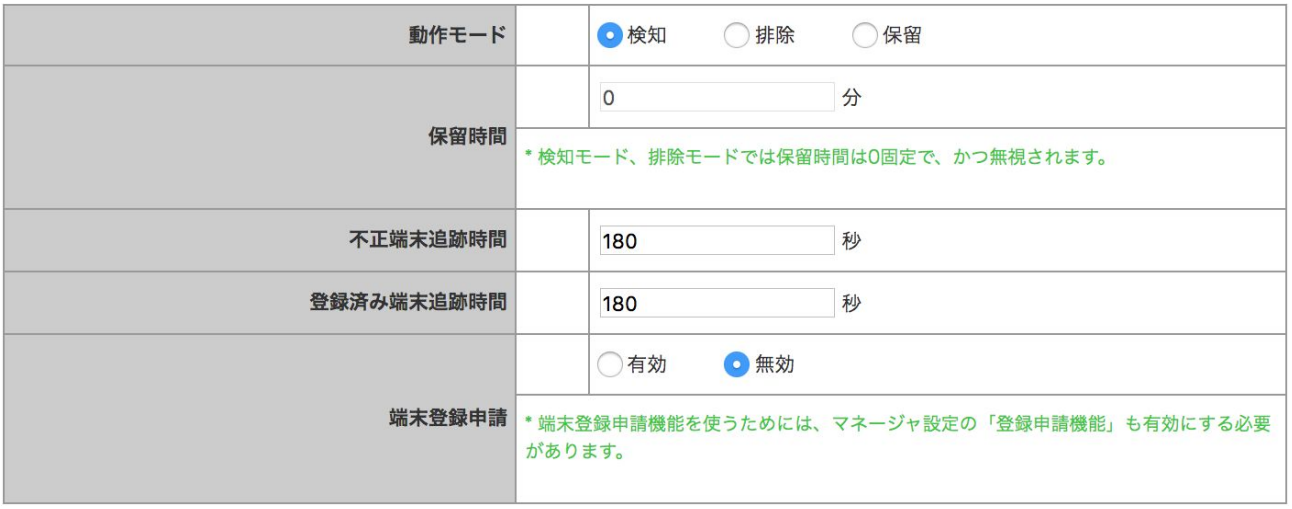
TIPS:
既存PCの登録は、【3.5.4　バックアップ/復元】の手順でCSVファイルをインポートして一括で行う事も可能です。

4.4 基本設定

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。

4.4.1 検知･排除方式

(1) メニューから[基本設定]をクリックします。
(2) 基本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[更新]ボタンをクリックすると、設定が変更/反映されます。



項目説明

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(動作モード:保留のみ)
不正端末追跡時間(秒)	不正接続PC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
登録済み端末追跡時間(秒)	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
端末登録申請	IntraGuardian2+ Manager Professionalの端末登録申請を使う際は[有効]にしてください。

- 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ください。
- 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、ルーターを必ず本製品に登録してください。

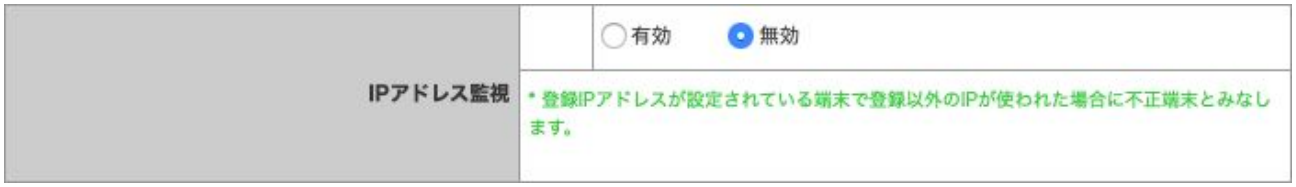
TIPS:

本製品に登録されていないPCを検知した場合、「不正接続一覧」に掲載されます。（動作モードが「排除」の場合、同時に該当する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」が更新されていきます。

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「不正接続一覧」から「端末履歴」に移します。なお、動作モードが「保留」の場合、初めてPCが検知されたときから「保留時間」以上経過した時に排除行動を始めます。

4.4.2 IPアドレス監視

LAN上のPCに固定IPを割り当てて運用している場合など、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時は不正接続と見なしたい場合があります。この場合、[有効]　にチェックしてください。



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）。

✴ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.4.3 IPアドレス変化検出

LAN上のPCのIPアドレスが変化したことを検出したければ[有効]にチェックしてください。このチェックが[無効]の場合は、IntraGuardian2+ Manager Professionalやメールでのイベントが通知されません。

✴ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.4.4 サブネットフィルタ機能

本製品は、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、出荷時は[有効]に設定してあります。なお、セカンダリIPを使用している場合は無効にしてください。サブネットフィルタ機能を無効にすると、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ようになります。(ただし、スイッチングハブなどにより、本製品に当該PCからのパケットが到達しない場合は検知できません)

サブネットフィルタ		◉ 有効　○ 無効

＊ 画面最下部の[確定]ボタンをクリックしたタイミングで反映されます。

4.4.5 例外IPアドレス登録機能

本機能を有効化すると、あらかじめ本製品に登録してあるIPアドレスの機器は不正端末として処理しなくなります。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)サーバーなどがある場合は有効にします。

例外IPアドレス		◉ 有効　○ 無効
例外レベル		○ 無視する　◉ 検知

例外IPアドレスに登録されているIPアドレスの機器を検知すると、自動的に登録済扱いになります。例外レベルが[無視する]の場合、自動登録イベントがマネージャに通知されません。

＊ 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と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、【5.4 例外IPアドレス一覧】をご覧ください。
＊ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

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あります。冗長化構成により、あらかじめ代替機の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形の運用を推奨します。ルーターなどの故障修理時、代替機のMACアドレスがわからない場合のみ、本機能を使用してください。

4.4.6 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利用		○有効 ●無効
優先プロトコル		●NetBIOS ○DNS

DNSによるコンピュータ名の取得を有効化した場合、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用するかを選択します。

- 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。
- 本機能のチェックを外しても、NetBIOSによるコンピュータ名の取得は止まりません。
- お客様の環境によっては、コンピュータ名を取得できない場合があります。
- コンピュータ名の取得はおおよそ30分に1度行います。
- 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.4.7 OS検出

OS検出を有効にすると、端末管理にOSの種類が表示されるようになります。

- ポートスキャンによりOS検出を実施しますので、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のみ有効化してください。

OS検出		○有効 ●無効

現在のバージョンでは、OSとしてWindows/Linux/Mac OS Xのみを検出します。
また、TYPE(用途)は、SSDPで検出した内容を出力します。

- 本機能による検出結果は推測値のため、誤検出が発生する場合があります。
- 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.4.8 IPv6機能

IPv6機能を有効にすると、IPv6の検知・排除も行われるようになりますが、排除可能なIPv6アドレスはMAC毎に2つまの対応となります。

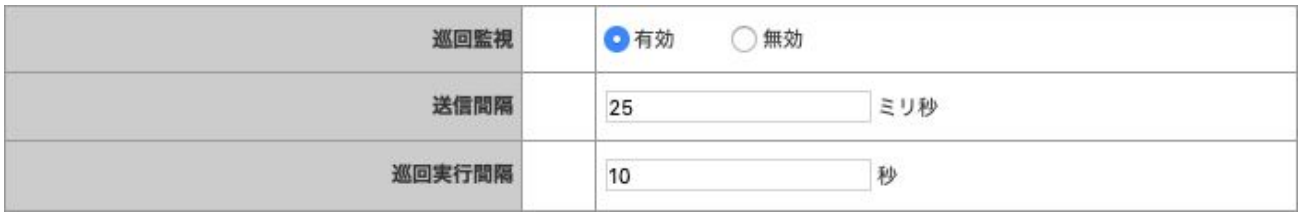
IPv6機能を有効にする		●有効 ○無効

- 本機能による検出結果は推測値のため、誤検出が発生する場合があります。
- 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.4.9 巡回機能

本製品は、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してあります。

(1) 巡回監視の[有効]にチェックを入れるとことで、巡回機能の有効/無効を切り替えます。
(2) 巡回機能を有効にする場合、合わせて下表の項目を設定します。



＊ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

項目説明

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ので、5ミリ秒以上に設定してください。
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使用する事を強く推奨します。

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に対する発行の完了後、巡回実行間隔で指定した時間だけ停止し、再度ARP要求パケットの送信を開始します。
例えば、クラスCのネットワークで上記の設定をした場合、

254 × 25msec+15sec = 21.35sec

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、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注意してください。

4.4.10 排除設定のカスタマイズを有効にする

排除パケットのカスタマイズ機能は、排除時のMACアドレスや、排除パケットの送信回数、送信間隔など細かく指定できます。特別に設定を変更しなければならない状態以外は、排除パケットのカスタマイズは有効にしないでください。

排除設定のカスタマイズ		○有効 ●無効
		* 登録IPアドレスが設定されている端末で登録以外のIPが使われた場合に不正端末とみなします。
不正端末宛ての排除パケット送信先MACアドレス (Ether Frame)		●ユニキャスト ○ブロードキャスト
不正端末宛ての排除パケットの送信元MACアドレス (ARP Packet)		○登録端末MACアドレス ●ダミーMACアドレス
		* 端末登録申請が有効の場合は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)		●ユニキャスト ○ブロードキャスト
不正接続端末への即時応答を有効にする		●有効 ○無効
不正接続端末への即時応答回数		2 回
不正接続端末への即時応答間隔		20 ミリ秒
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		●有効 ○無効
不正->不正への継続妨害間隔		1100 ミリ秒
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		●有効 ○無効
不正->登録への継続妨害間隔		1100 ミリ秒
正規端末宛ての排除パケットの送信元MACアドレス (ARP Packet)		●登録端末MACアドレス ○ダミーMACアドレス
		* 端末登録申請が無効の場合で、IntraGuardian2本体のMACアドレスを選択した場合にはダミーアドレスが使用されます。
正規端末宛ての排除パケットの送信先MACアドレス (ARP Packet)		●ユニキャスト ○ブロードキャスト
登録済み端末への即時応答を有効にする		●有効 ○無効
登録済み端末への即時応答回数		1 回
登録済み端末への即時応答間隔		1100 ミリ秒
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		●有効 ○無効
不正->登録への継続妨害間隔		1100 ミリ秒

＊ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.5 通知設定

本製品からのメールでの通知を受け取るための設定を行います。

4.5.1 メール通知設定

本製品の配信するメール通知に関する設定を行います。

(1) メニューから[メール通知設定]を押します。
(2) メール通知の[有効]にチェックを入れるとメール通知機能を有効化できます。

メール通知		○ 有効 ● 無効
メール件名		【IntraGuardian2】不正
言語		日本語
宛先		
SMTPサーバ		
ポート番号		
送信元		
SSL利用		○ 使用しない ● STARTTLS対応 ○ STARTTLS（証明書無視）
認証方式		● 使用しない ○ SMTP-AUTH ○ POP before SMTP
POP3サーバ		
ポート番号		
アカウント		
パスワード		
メール集約時間		10 秒
再送待ち時間		300 秒
最大再送回数		6 回
テスト送信		保存してテスト送信

✴ 画面最下部の[更新]ボタンをクリック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、あわせて下表の項目を設定します。

項目説明

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
SSL利用	利用しない/STARTTLSを利用する/STARTTLSで証明書エラーを無視 の3種類から選びます。
認証方式	メール配信に利用するSMTPサーバの認証方式 ＊ 対応認証方式: ・SMTP-AUTH(PLAIN、LOGIN、NTLM、CRAM-MD5、DIGEST-MD5) ・POP before SMTP
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

＊ パスワードに使える最大文字長は15文字です。

宛先、SMTPサーバ、ポート番号、送信元と認証方式の設定後に[保存してテスト送信]ボタンをクリックすると、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利用します。

TIPS:
テスト送信時は、詳細なログが[ログ]の画面に表示されます。
メールが送信できない場合にご活用ください。

4.5.2 IPアドレスの変化通知

本製品が登録PCのIPアドレスが変化したものを発見した時、メールで通知します。

(1) IPアドレスの変化通知の[有効]にチェックを入れてIPアドレス変化通知を有効化できます。通知を有効にする場合、あわせてメールの件名を設定します。

IPアドレス変化通知		○有効 ●無効
		* 基本設定のIPアドレス変化検出が無効の時は、メール送信もできません。
メール件名		IP変化

✴ 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していない場合、メール通知は行われません。
✴ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

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り、本機能で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、多くのメールが発送されます。

TIPS:
特定の登録PCだけIPアドレス変化の通知を行いたくない場合、該当PCの登録IPアドレスを空欄にしてください。詳しくは、【4.3 既存PCの登録】を参照してください。

4.5.3 コンピュータ名の変化通知

本製品がコンピュータ名の変化したPCを発見したとき、メールで通知します。

(1) コンピュータ名変化通知のラジオボタンで、コンピュータ名変化通知の有効／無効を切り替えます。

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。

(2) 通知を有効にする場合、あわせてメールの件名を設定します。

コンピュータ名変化通知		○有効 ●無効
メール件名		コンピュータ名変化

✴ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.5.4 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) 稼働通知のラジオボタンで、稼働通知の有効／無効を切り替えます。
(2) 稼働通知を有効にする場合、あわせて下表の項目を設定します。

✶ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

項目説明

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:
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個別に指定することはできません。

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、管理マネージャを別途入手して利用してください。

4.5.5 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。
(2) イベント通知を有効にする場合、あわせてメールの件名を設定します。

イベント通知を有効にする		○有効　●無効
メール件名		イベント通知
例外IPアドレスの通知		●無視　○検知

＊ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

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」
例外IPアドレスの通知を有効にすると、次の内容のメールが送信されます。
・「例外IPアドレスが登録されました」

4.5.6 SNMPトラップ通知

本製品が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) メニューから[SNMP設定]を押します。
(2) SNMPトラップ通知のラジオボタンで有効/無効を切り替えます。
(3) トラップ送信先のアドレスとコミュニティ名を指定し、次からの表で通知を受けたいイベントを選択します。

SNMPトラップ通知		○有効　●無効
トラップ送信先		
コミュニティ名		

＊ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.5.7 不正接続検知を通知する

本製品が不正接続を検知した時、SNMPトラップを送信します。

(1) 不正接続検知通知のラジオボタンで通知の有効/無効を切り替えます。
(2) 通知を有効にする場合には、あわせてOIDを設定します。

不正接続検知通知		○有効 ●無効
OID		.1.3.6.1.
可変引数1 タイプ		●使用しない ○INTEGER ○STRING
可変引数1 OID		.1.3.6.1.
可変引数1 値		
可変引数2 タイプ		●使用しない ○INTEGER ○STRING
可変引数2 OID		.1.3.6.1.
可変引数2 値		

＊ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.5.8 不正接続検知が無くなったことを通知する

本製品による不正接続検知が無くなった場合、SNMPトラップを送信します。

(1) 不正接続解除通知のラジオボタンで、通知の有効/無効を切り替えます。
(2) 通知を有効にする場合、あわせてOIDを設定します。

不正接続解除通知		○有効 ●無効
OID		.1.3.6.1.
可変引数1 タイプ		●使用しない ○INTEGER ○STRING
可変引数1 OID		.1.3.6.1.
可変引数1 値		
可変引数2 タイプ		●使用しない ○INTEGER ○STRING
可変引数2 OID		.1.3.6.1.
可変引数2 値		

＊ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.5.9 IPアドレスの変化を通知する

本製品が登録機器のIPアドレス変化を検知した時、SNMPトラップを送信します。

(1) IPアドレス変化通知のラジオボタンで、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、基本設定画面の[IPアドレス変化検出]を有効にしていないと通知は行なわれません。

(2) 通知を有効にする場合、あわせてOIDを設定します。

IPアドレス変化通知		○有効 ●無効
		* 基本設定のIPアドレス変化検出が無効の時は、SNMPトラップ送信もできません。
OID		.1.3.6.1.
可変引数1 タイプ		●使用しない ○INTEGER ○STRING
可変引数1 OID		.1.3.6.1.
可変引数1 値		
可変引数2 タイプ		●使用しない ○INTEGER ○STRING
可変引数2 OID		.1.3.6.1.
可変引数2 値		

- ✶ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.5.10 コンピュータ名の変化を通知する

本製品がコンピュータ名の変化したPCを発見した時、SNMPトラップを送信します。

(1) コンピュータ名変化通知のラジオボタンにて有効/無効を切り替えます。
(2) 通知を有効にする場合には、あわせてOIDを設定します。

コンピュータ名変化通知		○有効 ●無効
OID		.1.3.6.1.
可変引数1 タイプ		●使用しない ○INTEGER ○STRING
可変引数1 OID		.1.3.6.1.
可変引数1 値		
可変引数2 タイプ		●使用しない ○INTEGER ○STRING
可変引数2 OID		.1.3.6.1.
可変引数2 値		

- ✶ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.5.11 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。

(1) 稼働通知ラジオボタンで通知の有効/無効を切り替えます。
(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。

稼働通知		○ 有効 ● 無効
OID		.1.3.6.1.
可変引数1 タイプ		● 使用しない ○ INTEGER ○ STRING
可変引数1 OID		.1.3.6.1.
可変引数1 値		
可変引数2 タイプ		● 使用しない ○ INTEGER ○ STRING
可変引数2 OID		.1.3.6.1.
可変引数2 値		

＊ 画面最下部の[更新]ボタンをクリックしたタイミングで反映されます。

4.5.12 イベント通知を有効にする

本製品が起動した時など、イベントが起こった時にSNMPトラップを送信します。

(1) 稼働通知ラジオボタンで通知の有効/無効を切り替えます。

稼働通知		○ 有効 ● 無効

＊ 画面最下部の[更新]ボタンをクリック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は固定です。

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。

TIPS:

起動	:	OID .1.3.6.1.6.3.1.1.5.1
エンジン再起動	:	OID .1.3.6.1.6.3.1.1.5.2
リンクアップ	:	OID .1.3.6.1.6.3.1.1.5.4

5 運用上の機能説明

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。

5.1 端末管理

本製品に登録されているPCの一覧を表示します。

(1) メニューから[端末管理]をクリックします。
(2) 本製品に登録されているPCの一覧が表示されます。

5.1.1 新しいPCの登録

本製品へ新たな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]ボタンをクリックします。
(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]ボタンをクリックすると、登録ユーザーの情報が新しい内容へ変更されます。

✶ [全てのVLANに登録]ボタンはVLAN版製品のみに表示されます。

項目説明

名称	登録するPCの名称 ","(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 ✶ 全てのオクテットが00またはFFは登録できません。
IPアドレス	登録する PC のIPアドレス 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 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。

✶ [基本設定]で　IPアドレス監視機能を有効にしている場合、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:
PCの登録は、最大40000件までできます。
VLAN版はVLAN毎に40000件です。

TIPS:

本製品をIntraGuardian2+ Manager Professional等の管理ソフトウェアと組み合わせて運用している場合、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ってください。

TIPS:

本製品をIntraGuardian2+ Manager Professionalと組み合わせて運用している場合、登録PCの情報はManagerが動作しているPCのストレージデバイス内に保存されます。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と通信できなかった場合、前回Managerから受け取ったデータを確認できれば、60秒後に動作をはじめます。なお、SKYSEA ClientViewと連携している際は、動作はしません。

5.1.2 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]ボタンをクリックします。

(2) 登録済みPC編集画面へ移動するので、変更する項目へと新しい内容を入力します。

項目説明

名称	登録するPCの名称 "","(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。 ＊ 全てのオクテットが00またはFFは登録できません。
IPアドレス	登録する PC のIPアドレス 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 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。
IPアドレス変化を通知しない/ ホスト名の変化を通知しない	IPアドレス変化やホスト名変化の通知を行うか、行わないかを指定します。

(3) [更新]ボタンをクリックすると、登録済みPCの情報が新しい内容へ変更されます。

5.1.3 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にチェックを入れます。

- 複数のPCを削除する場合には、複数のチェックボックスにチェックを入れます。

(2) 表の左上または左下にある[選択削除]ボタンをクリックすると、チェックしたPCが削除されます。

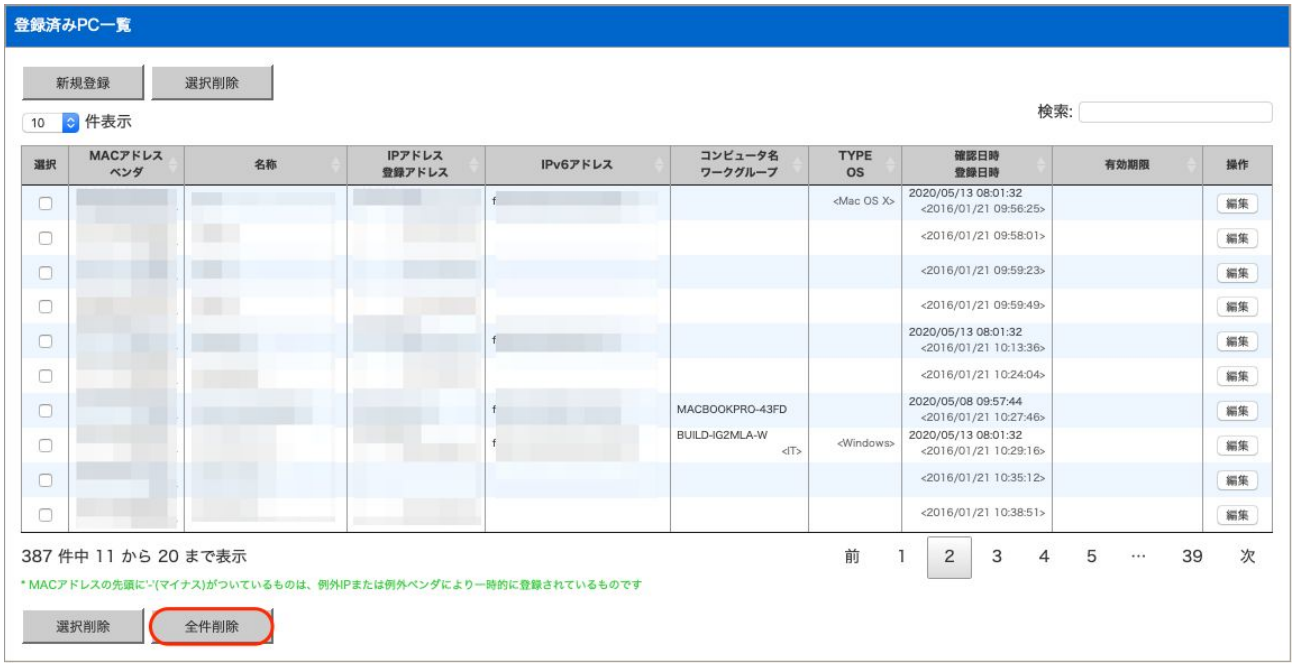
- 本製品の登録から削除されたPCは、削除後すぐに検知/排除の対象となります。
- どちらの[削除]ボタンを押しても動作に違いはありません。

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

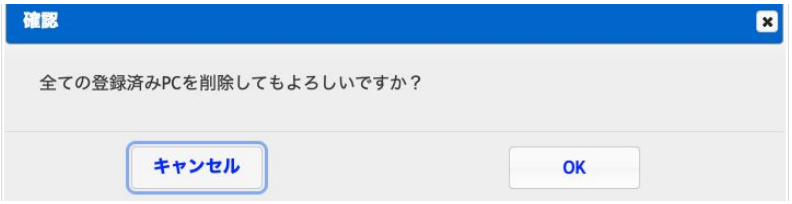
5.1.4 登録済みPCの全件削除

本製品へ登録されている全PCを削除します。

(1) 一覧の下にある[全件削除]ボタンをクリックすると、確認画面が表示されます。



(2) [OK]をクリックすると、登録されているPCがすべて削除されます。



5.2 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]をクリックします。
(2) 不正接続PCの一覧が表示されます。

5.2.1 PCの登録

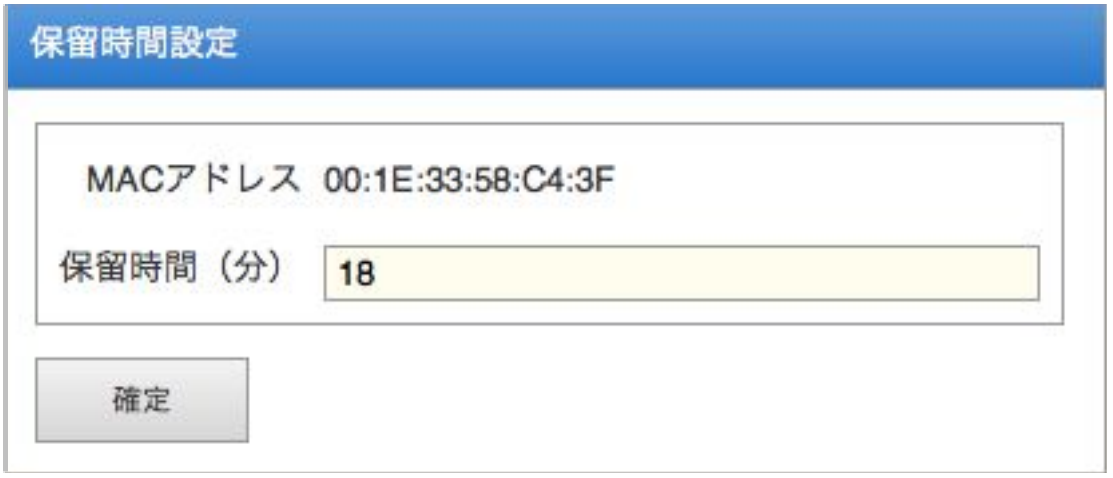
一覧に表示されているPCを、個別に本製品へ登録します。

(1) 登録したいPC欄にある[登録]ボタンをクリックします。
  ✴ 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登録画面へ移動するので、【5.1.1 新しいPCの登録】と同様に、本製品へPCを登録します。

5.2.2 保留時間の変更

動作モードが[保留]になっているとき、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]ボタンをクリックします。
(2) 保留時間設定画面へ移動するので、保留時間を分単位で入力し、[確定]ボタンをクリックします。



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。例えば「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。

5.2.3 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。

(1) [全件登録]ボタンをクリックすると、確認画面が表示されます。

(2) [OK]ボタンをクリックすると全PCが登録されます。

5.3 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[端末履歴]をクリックします。
(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。

5.3.1 PCの登録

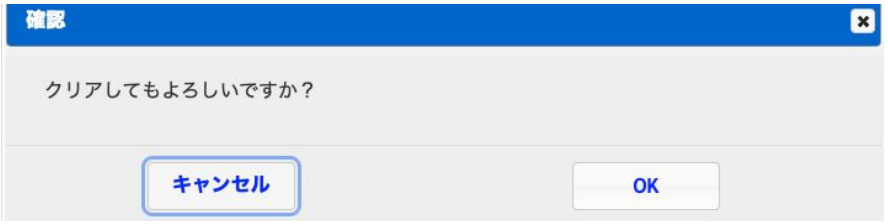
検知履歴に表示されているPCを、個別に本製品へ登録します。

(1) 登録したいPC欄にある[登録]ボタンをクリックします。
✶ 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登録画面へ移動するので、【5.1.1 新しいPCの登録】と同様に、本製品へPCを登録します。

5.3.2 検知履歴のクリア

検知履歴の内容をクリア(全消去)します。

(1) 最下部にある [クリア]ボタンをクリックすると、確認画面が表示されます。
(2) [OK]をクリックすると、検知履歴がクリアされます。



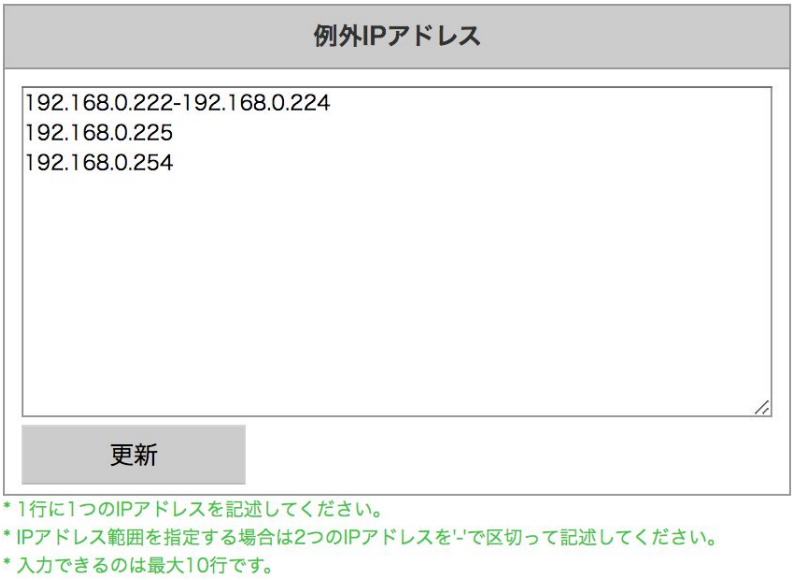
TIPS:

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。

5.4 例外IPアドレス

不正PCとして検知・排除する対象から除外する機器の、IPアドレス登録一覧を作成します。

(1) メニューから[例外アドレス]をクリックします。
(2) 上部に例外IPアドレスの一覧が表示されます。



5.4.1 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アドレスが一覧されているフィールドに、新たにアドレスを入力します。
範囲の場合は、192.168.0.1-192.168.0.10のようにハイフン区切りで入力します。
(2) 入力が完了したら[更新]ボタンをクリックしてください。

✴ 基本設定画面で例外IPアドレスを有効にしていない場合、本画面で登録された内容は一切機能しません。

TIPS:
例外IPアドレスは最大で10件まで登録できます。
例外IPアドレスは範囲で入力することもできます。

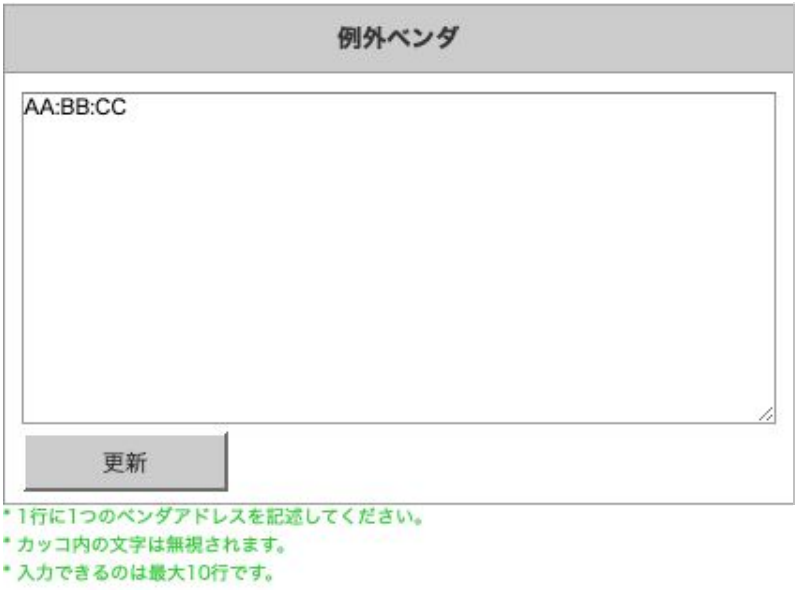
5.4.2 例外IPアドレスの削除

登録されている例外IPアドレスを削除をするには、フィールドで不要なアドレスを削除してから[更新]ボタンをクリックしてください。

5.5 例外ベンダー一覧

不正PCとして検知・排除する対象から除外する機器を、MACアドレスの上3桁で指定することができます。

(1) メニューから[例外アドレス]をクリックします。
(2) 下部に例外ベンダーの一覧が表示されます。



5.5.1 例外ベンダーの登録

例外ベンダーを本製品に登録します。

(1) 例外ベンダーのフィールドにMACアドレスの上3桁をコロン区切りで入力してください。
(2) [更新]ボタンをクリックして登録します。

5.5.2 例外ベンダーの削除

登録されている例外ベンダーを削除するには、フィールド内の不要な行を削除してから[更新]をクリックしてください。

TIPS:
例外ベンダーの横に表示されるベンダー名は表示されているだけです。

5.6 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。

TIPS:

IntraGuardian2+EXは、3.5系まで各VLAN毎に異なるユーザー名とパスワードを割り当てられましたが、本バージョンから一元管理されるようになりました。バージョンアップした場合は、初期パスワードに戻りますので新たに設定しなおしてください。

5.6.1 ユーザーの追加登録

(1) 右上のメニューから[アカウント]をクリックします。
(2) メニューから[アカウント設定]をクリックしてください。
(3) ユーザーの一覧が表示されるので、一覧表の左上の[新規登録]ボタンをクリックします。

(4) 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。
(5) [確定]ボタンをクリックすると、新しいユーザーが増えます。

項目説明

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。

5.6.2 ユーザーの編集

ユーザーの一覧表にある[編集]ボタンをクリックすると、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、パスワード欄と再入力欄を空欄にした状態で[確定]をクリックします。

5.6.3 ユーザーの削除

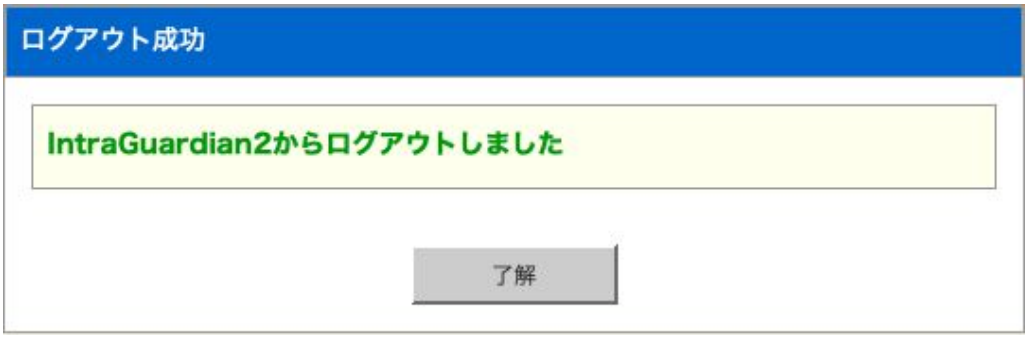
ユーザーの一覧表のチェックボックスにチェックを入れて[削除]ボタンをクリックすると、選択したユーザーを削除することができます。

＊ 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。

5.7 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]をクリックします。
(2) ログアウトすると、以下の画面が表示されます。



(3) [了解]ボタンをクリックすると、ログイン画面へ移動します。

改訂履歴

2016-03-03	初版	
2016-04-14	第2版	・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 ・VCCI-A対応記述の追記
2016-08-17	第3版	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	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	バージョン番号の更新
2018-01-24	第6版	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	・管理ポート設定の文言「デフォルトゲートウェイにする」を「代表のゲートウェイにする」に変更 ・動作設定の文言「サブネットフィルタ機能を無効にする」を「…機能を有効にする」に変更
2018-10-03	第8版	・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
2018-12-17	第9版	・P.56,59 端末登録の説明欄に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
2019-01-21	第10版	バージョンアップに伴い表紙のバージョン番号と版数を変更
2020-05-13	第11版	Ver.3.6.0 向けに変更 それに伴い、03PLとEXのマニュアルの統合

IntraGuardian2+ EX
Version 3.6.0 ～

スタートアップガイド

2020年5月22日

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

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