# IntraGuardian2 note： 追跡時間と保留時間

2009 年 12 月 1 日
日本シー･エー･ディー株式会社

## 追跡時間

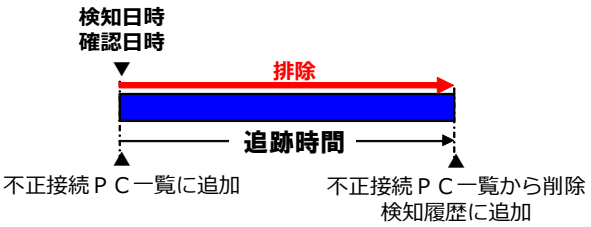
イーサネットにおいては、ある PC がネットワークから離れる際に何らかの信号を出すということが無いので、一定時間パケットを発信していない事によってしか PC がネットワークからいなくなった事象を捉えることができません。

**IntraGuardian2** では、この「一定時間」の事を「追跡時間」と呼んでいます。


図 1　GUI 画面 ［動作設定］ 排除モードの場合


図 2　GUI 画面 ［動作設定］ 保留モードの場合

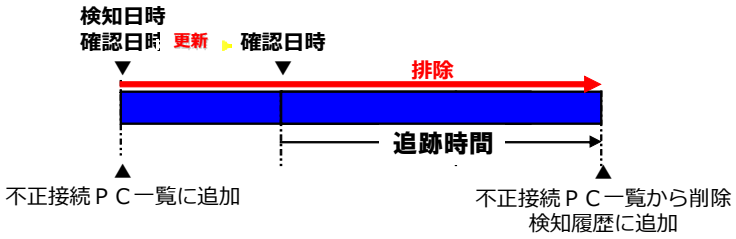
ある PC から発信されたパケットを **IntraGuardian2** が受信した時、**IntraGuardian2** はその PC の「確認日時」を更新します。そして、「確認日時」から「追跡時間」以上経過している PC があれば、「追加時間」継続して、その不正 PC の存在を探しつづけたものの、検知できなかったことにより、その PC がネットワークから離れたと判断するのです。




**IntraGuardian2** は、ネットワーク上のパケットを発見すると、その MAC アドレスが登録されたものである場合、登録 PC 一覧表内の「確認日時」を更新します。

登録された MAC アドレスではない場合、不正 PC として既に「不正接続 PC 一覧」にリストアップされている MAC ア

ドレスがあれば、その「確認日時」を更新します。「不正接続 PC 一覧」になければ、新たに検知された不正 PC として、その MAC アドレスをリストアップし、「検知日時」と「確認日時」を書き込みます。




さらに、**IntraGuardian2** は定期的に「不正 PC 一覧表」を確認し、「確認日時」から「追跡時間」以上が経過した MAC アドレスが無いかをチェックします。「追跡時間」以上経過したリストは、既にネットワークには存在しないと判断し、その記録を「不正接続 PC 一覧」から削除し、「検知履歴」にリストアップします。

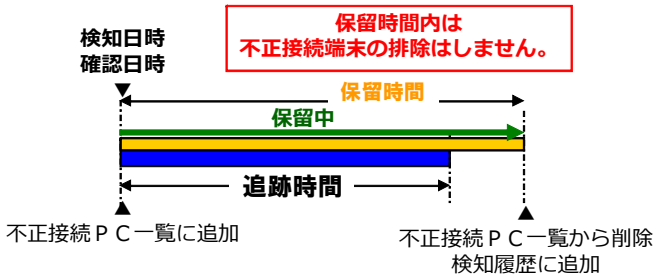
このようにして、「不正接続 PC 一覧」には、“現在ネットワーク上にある PC であり、**IntraGuardian2** 登録されていないもの”が掲載されることになります。

## 保留時間

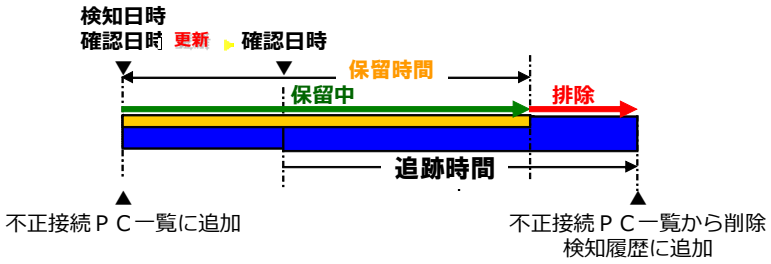
**IntraGuardian2** を「排除モード」で運用している場合、「不正接続 PC 一覧」にリストアップされている不正 PC の通信を妨害する ARP パケットを投げ続けます。

このとき、“**IntraGuardian2** が不正 PC を検知してから、一定時間は通信妨害を行なわないで様子をみる”という動作をさせたい場合、「保留モード」を使います。「保留モード」は、“不正 PC の排除を保留する”モードです。この、通信妨害を保留する時間の事を「保留時間」と呼びます。

「保留時間」には、一般には「追跡時間」よりも長い時間を設定します。ネットワーク管理者はその時間以内に接続 PC 利用の可否を判断し、登録をする、その PC の保留時間をゼロにする（排除する）、その PC の保留時間を長くする、などの処置を行ないます。




「保留時間」は「検知日時」（「不正接続 PC 一覧」にリストアップされた日時）を起点としています。（「追跡時間」が「確認日時」を起点としているのと異なる点にご注意ください。）




**保留時間の起点は検知日時であり、検知日時は更新されません。**
**追跡時間の起点は確認日時であり、追跡時間内にて不正 PC を検知する度に確認日時は更新されます。**

なお、「保留時間」内にある PC については、「追跡時間」が経過しても不正 PC 一覧表から削除しない仕組みになっています。

以上

---

本仕様説明は、発行日現在にてリリースされている **IntraGuardian2** を基準とするものです。機能追加及び変更等による仕様の変更がある場合がございます。