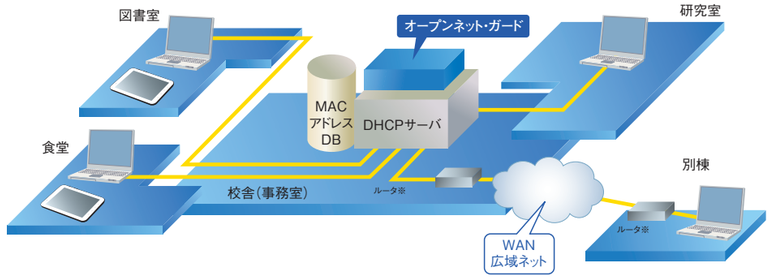
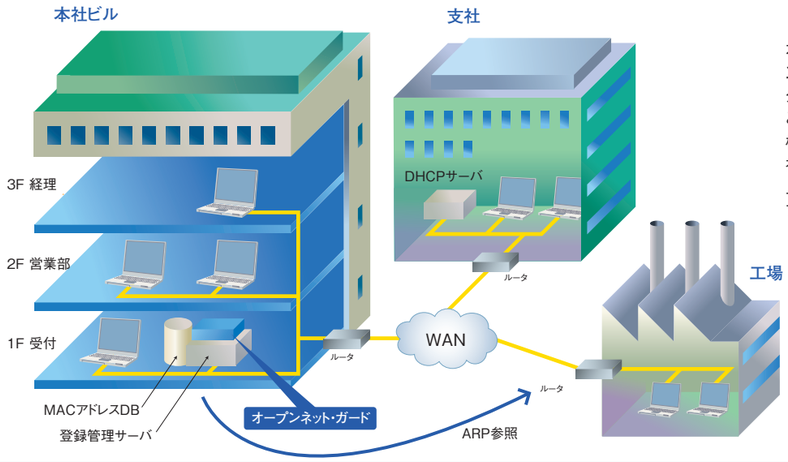
■大学キャンパスでの適用例（MAC認証DHCP）



キャンパスネットワークにオープンネット・ガードを導入。学生はMACアドレスを登録すると教室、図書室や食堂、研究室などで煩雑な接続設定をせずにネットワークを利用できます。また、広域ネット（WAN）を介した別棟でも利用できます。
また、タブレット端末などもMACアドレスを登録することにより、利用することができます。

■企業での適用例（不正接続検知）



本社に登録管理サーバを導入、各セグメントのデフォルトゲートウェイにあたる、ルータやL3スイッチから、ARP情報を取得することにより、ネットワークに接続されている機器を把握できます。本社はもちろん、支社や工場など、WANを介したネットワーク上の不正機器も検知し、管理者の方にアラートメールを送信します。

■システム構成

オープンネット・ガードのホームページをご覧ください。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/ong/

S03K-04-12 | 2019.11

HITACHI
Inspire the Next

不正接続防止ソリューション

オープンネット・ガード

MACアドレス認証型セキュリティ
不正接続機器の検知と遮断

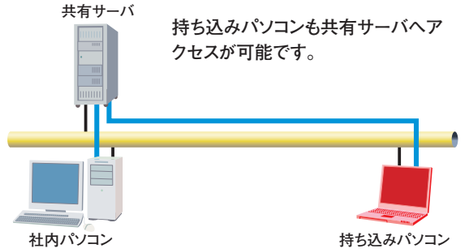
株式会社 日立ソリューションズ

MAC Address Registered
オープンネット・ガード

MACアドレス管理は、ネットワークのセキュリティ確保の第一歩です

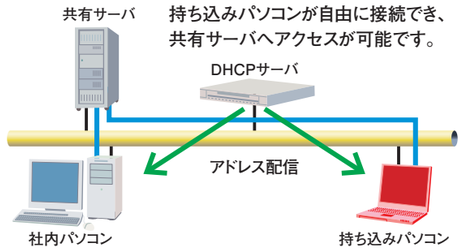
近年、様々な機器を容易に接続できる便利さの反面、ネットワーク管理者の目の届かない所で、私用パソコンを接続され、データを持ち出されるリスクも増大しています。オープンネット・ガードはMACアドレスを管理し、豊富なセキュリティ機能により、セーフティなネットワーク環境を実現します。また、強力なMACアドレスの管理機能で、システムの導入・運用を支援します。

● 固定IPでの運用



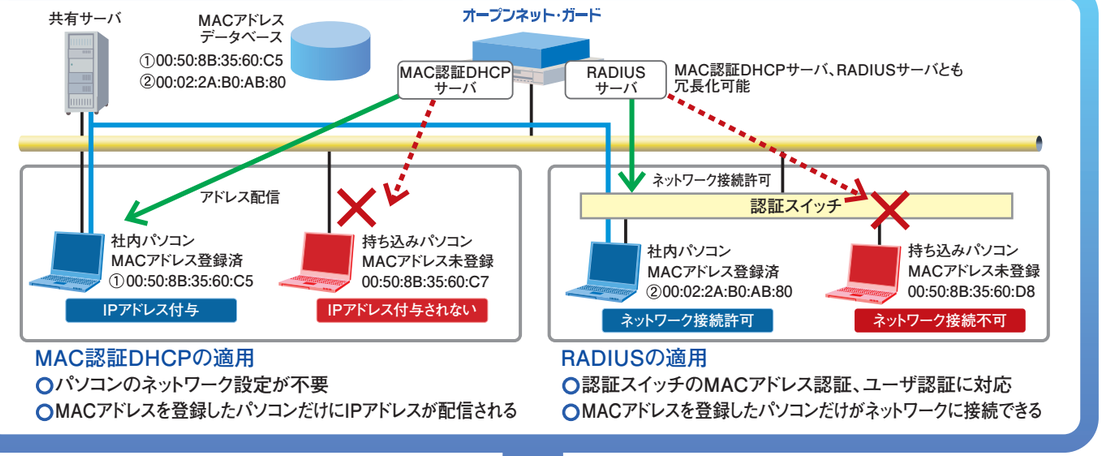
✕IPアドレスの管理が大変
✕パソコンの移設時に、ネットワーク設定の変更が必要

● DHCPサーバでの運用



○パソコンのネットワーク設定が不要
✕不正接続を防止できないため、セキュリティレベルが低下

● オープンネット・ガードでの運用



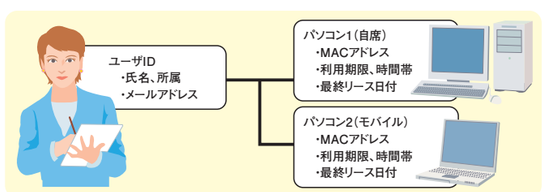
MAC認証DHCPの適用
○パソコンのネットワーク設定が不要
○MACアドレスを登録したパソコンだけにIPアドレスが配信される

RADIUSの適用
○認証スイッチのMACアドレス認証、ユーザ認証に対応
○MACアドレスを登録したパソコンだけがネットワークに接続できる

◎ MACアドレス認証により、ネットワークのセキュリティを格段にアップ!
◎ ユーザID、MACアドレスのかんたん管理により、TCOを削減します!

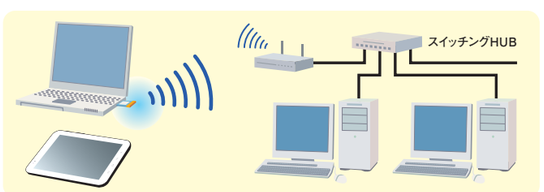
＋ かんたん管理-1　ユーザIDとMACアドレスの連携

ユーザIDとMACアドレスをリンクして管理しています。一人で複数台のパソコンを利用する場合でも、ユーザIDを無効にすると、関連する全てのMACアドレスが無効になります。



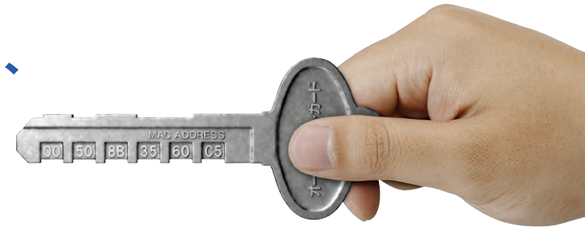
＋ かんたん管理-2　接続形態を選びません

MACアドレスが登録されたパソコンは無線LAN、有線LANに関係なくLANに接続できます。



※ 1台のマシンで有線/無線LANを使用する場合には、ライセンスが2つ必要になります。

日本生まれのオープンネット・ガード、ユーザーフレンドリーなGUIでかんたん管理をサポートします。



MACアドレス情報管理

登録情報一覧画面　　新規登録情報画面

● **ハードウェア情報**
MACアドレスとベンダ名称を表示
DHCP配信対象外の設定が可能

● **ユーザ情報**
ユーザIDとユーザ名、組織を表示
端末利用者の管理が可能

● **コンピュータ情報**
ホスト名、利用OS、管理番号、備考を表示

● **利用期間**
MACアドレスの利用可能期間、時間帯を指定

RADIUS連携機能

管理しているMACアドレスやユーザIDから、認証サーバの定義を生成し、認証スイッチと連携します。複数メーカーの認証スイッチが混在するネットワークにも容易に対応可能です。MACアドレス認証または、ユーザ認証により、不正な機器の通信を遮断できます。

Infoblox連携機能

Infoblox社のNIOSを搭載した機器をDHCPサーバとして使用する場合、MACアドレスおよび、固定配布のIPアドレスをオープンネット・ガードで管理し、InfobloxのDBへ動的に反映することができます。
また、既設のInfobloxを使用する場合、InfobloxからMAC情報を取得することができ、容易にMAC管理と不正検知機能を既存Infoblox環境に適用することができます。

IntraGuardian2連携機能

日本シー・エー・ディー株式会社のIntraGuardian2を不正接続検知／排除装置として使用する場合、オープンネット・ガードで管理しているMACアドレスおよび、固定配布のIPアドレスをMACグループ単位でIntraGuardian2へ反映することができます。
また、複数のIntraGuardian2をオープンネット・ガードで一元管理でき、設定の一括変更にも対応しています。
※ IntraGuardian2 EXにも対応。(1VLANにつき1台分のIG2ライセンスを使用します)

不正接続監視機能

PING方式

DHCPサーバからのPINGを利用した不正接続監視機能です。
DHCPサーバから払い出されていない不正なIPアドレスを検知することができ、設定した監視範囲にDHCPサーバからPINGを発行して監視を行います。

※PINGに応答しないPC(機器)の検知はできません。

ARP方式

ルータのARP情報を利用した不正接続監視機能です。
未登録のMACアドレスを検知することができ、ARP情報を取得する前に、検知用パケット(PING,TCPパケット,UDPパケット)をIPレンジに発行することで、PINGに応答しないPC(機器)も検知することができます。また、ジュニパーネットワークス社のファイアウォール製品 SSG/SRXシリーズと連携し、遮断することができます。

IntraGuardian2方式

日本シー・エー・ディー株式会社のIntraGuardian2を各セグメントに設置して、不正接続端末を検知／排除(通信遮断)する機能です。
MACアドレスとIPアドレスの組合せチェックもできます。

※検知・排除・保留の動作はIntraGuardian2側の設定に依存します。

SNMPトラップ送信機能

SNMPトラップ送信機能により、DHCPサーバやRADIUSサーバに障害が発生した場合や回復した場合、不正接続を検知した場合などに、SNMPトラップ送信による通知ができます。
これにより、様々なネットワーク管理システムを使用して、オープンネット・ガードの状態を監視することができ、迅速な障害対応が可能になります。

さらに、強力なセキュリティ管理の実現へ　日立ソリューションズでは、ネットワーク・セキュリティ・ソリューション製品との組合せにより、さらに万全なネットワーク環境のご提案も行っています。