不正PC検知・排除システム

L2Blocker

「不正接続防止ツール」市場
累計導入実績
No.1

EX NET WORKS GEN
USE INNOVATIVE TECHNOLOGY.

出典:株式会社富士キメラ総研「情報漏洩対策需要に沸く不正接続防止ツール市場2017」

L2Blocker

社内LANへの未認可機器、不正接続を検知・遮断

✔ 私物スマートフォン対策

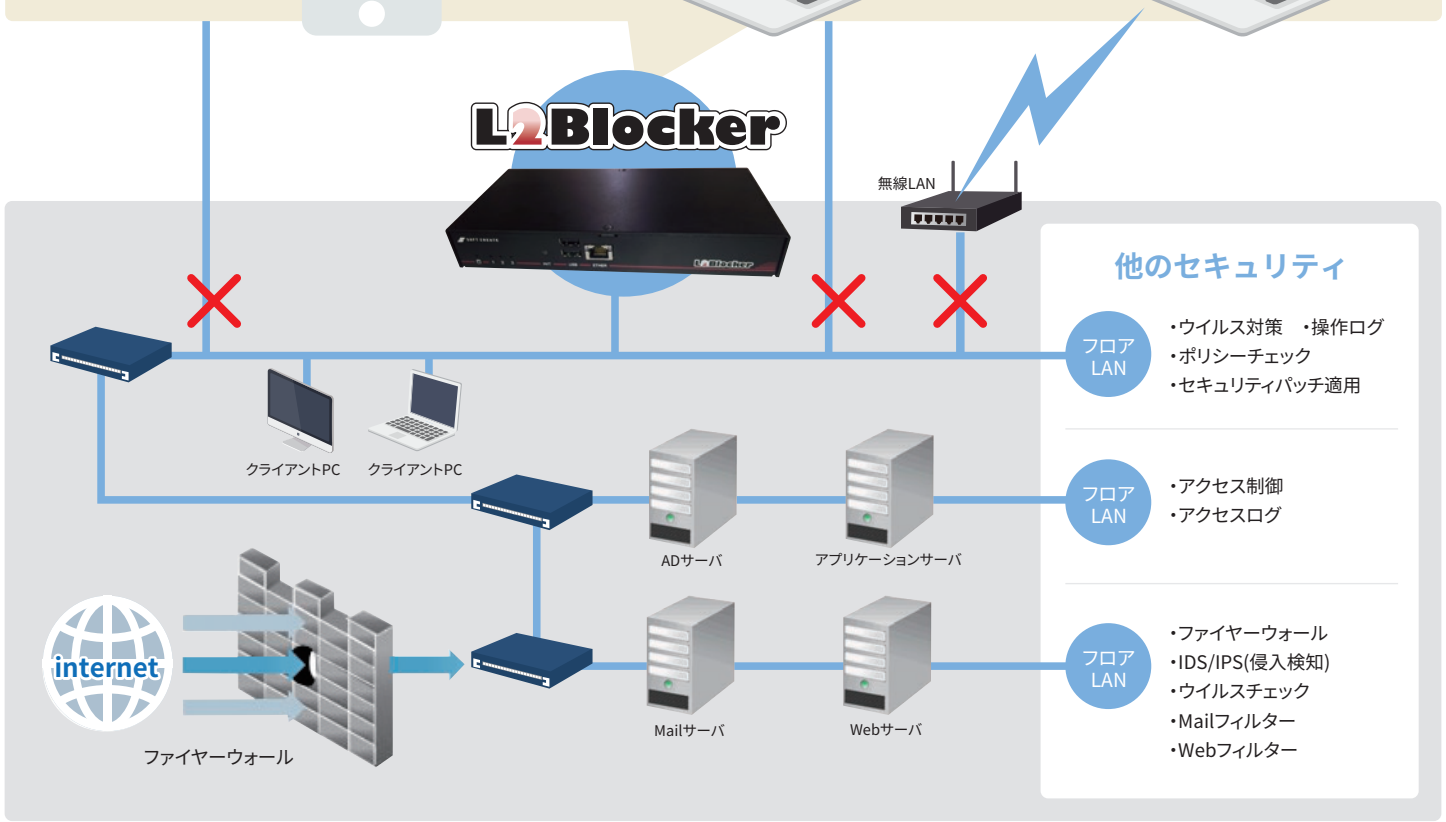
スマートフォンを社内ネットワークにつなげられ、インターネット回線に負荷が出たり、DHCPが枯渇することを防止

✔ 持込みPC対策

社員の自宅PCや、業者のPCなどを自由に接続させない

✔ 不正アクセス遮断

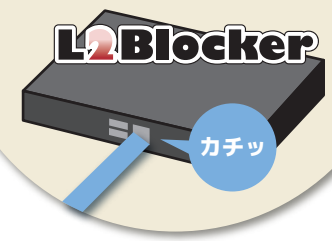
WEPなどを解析し、外部PCが社内ネットワークへ接続するのを防止



他のセキュリティ

既存LAN変更なし

既存LANにセンサーを接続するだけで、導入できます。
※既存LANに影響はなし



情報漏洩対策

Mailフィルターや USBメモリを禁止しても、私物PCの接続を禁止しなければ情報漏えいは防げません。

24時間365日監視

アプライアンス機器だから、24時間365日検知・排除を行います。

L2Blockerによる課題解決シーン

社内での端末利用状況が不明

セキュリティ対策を行う上で、IT機器の把握は必要です。
部門で購入した機器や個人の持ち込み機器等の存在を明からにすることが可能です。

**情報収集モードで
社内のIT機器を見える化**

不明機器による不正な接続を防止したい

管理されていない端末のネットワーク利用は、ウィルスに感染、脆弱性に対する対策がされていない等のリスクが内在している可能性があるため、ネットワークを利用させるのは危険です。

**許可登録されていない
機器の接続を遮断**

台数が多いIT機器の棚卸しが大変

IT機器も会社の資産です。使用されない遊休資産、廃棄や紛失したIT機器があれば、正確な資産状況が把握できないだけではなく、セキュリティ面でも問題が生じます。IT機器が利用されていることを検知日時で常に確認する事ができます。

**最終検知日時で
IT機器を棚卸し**

無線LANのセキュリティ対策をしたい

無線LAN環境の導入は、業務効率化に重要な役割を果たしています。アクセスポイントの台数が増えてくると、接続許可端末の登録や削除等のメンテナンスにかける運用維持に膨大な時間が掛かってしまいます。
L2Blockerなら有線・無線の接続を許可する端末を一元管理し、セキュリティ対策が行えます。

※アクセスポイントはブリッジモードで動作していることが条件です。

**有線・無線の
接続許可端末を一元管理**

IT資産管理で漏れがないか確認したい

IT資産管理を徹底するためには管理対象端末にエージェントソフトがインストールされている必要があり、漏れがあった場合は管理を徹底することができません。
L2Blockerの情報収集機能と連携させることで、管理漏れの端末を発見し、是正させることができます。

**IT資産管理連携で
管理漏れを把握・是正**

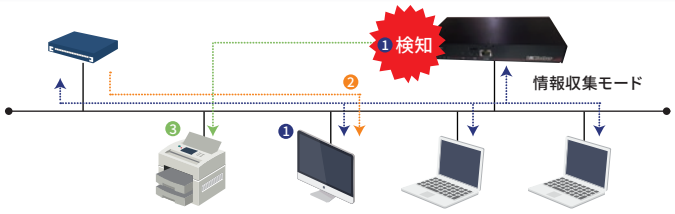
マルウェア等の感染時に緊急対応したい

日々巧妙化、複雑化するサイバー攻撃に対して完全防御が難しく、感染に気がつかないケースが増加しています。振る舞い検知ソリューションと組み合わせることで、感染の疑いが見つかった端末をIPアドレスから検索し、遠隔地からでも強制的にLANの擬似的抜線を行えます。

**許可登録されている機器でも
強制的に切断**

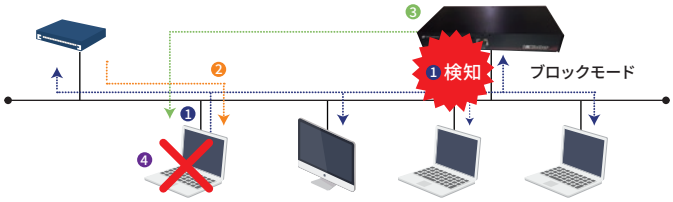
L2Blocker機能紹介

情報収集

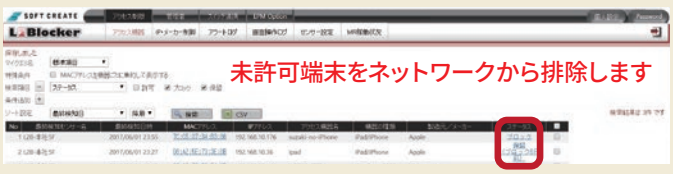


❶ARPリクエストによりゲートウェイを確認（検知）
❷ リクエストを受けたゲートウェイが返信
❸ センサーが探索しリクエストを出さない機器も検知

ブロック



❶ARPリクエストによりルーターのMACアドレスの確認を依頼
❷ 問い合わせを受けたルーターが自身のMACアドレスを返信
❸ センサーが不正接続と判定した場合ブロックパケットを返信
❹ 不正に接続された端末は通信ができない



アクセス機器管理

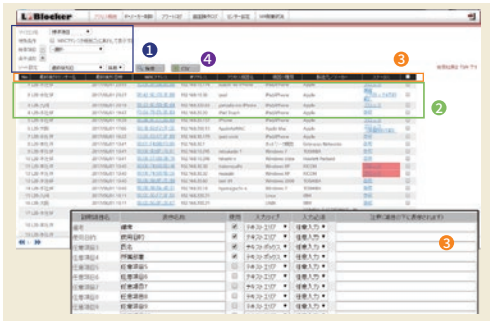
ネットワーク上の機器を把握

❶ 検索
表示されている項目にて特定の機器の検索が可能

❷ 自動収集
・MAC アドレス
・IPアドレス
・アクセス機器名
・メーカー名
・機器種別判定

❸ 管理画面
利用状況に合わせて表示項目の変更、追加が可能

❹ 管理画面
登録データの入出力が可能



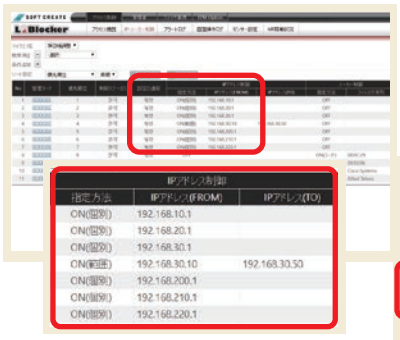
※情報収集機能のアクセス機器名機能と機器の種別判定は補足機能であり、全ての情報が取得できることを保証するものではありません

ステータス変更履歴の確認

登録されている機器の現在のステータスをクリックすることで、過去登録時から現在に至るまでの変更履歴を確認できます。
またステータスの変更も管理者による変更か、他製品連携による変更かも記録されているため、なぜ変更されたか把握することが可能です。

IP アドレス制御

IP アドレスでの許可とブロック



●IPアドレス制御・許可
登録IPアドレスに対して、許可・不許可の設定が可能です。
IP アドレスは、個別もしくは範囲でも選択が可能です。

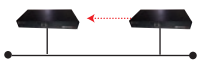
●重要なネットワーク機器を遮断しないようにネットワーク機器に割り当てられているIPアドレスを登録する事で MAC アドレスの登録の有無に関係なく遮断を行いません。

※ポリシー制御レコードの合計数は5,000 レコードまで

センサー管理

センサーの冗長化

バックアップ機がメインを監視し、障害があれば自動で切り替わります。



マネージャー配下で稼働中のセンサー管理画面で、各センサーの動作モード（収集・保留・ブロック）と稼働状況を確認できます。センサーを２台､同セグメントにご用意頂くことで､1台をバックアップ機として冗長化構成を組むことが可能です。

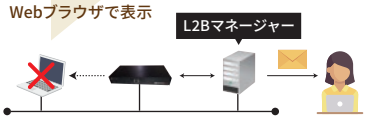
管理画面ではホスト名１つに対して MAC アドレスが２つ表示され、グレー表示がバックアップ機を表します。

L2Blocker機能紹介

ブロック通知＆申請機能

ブロックされた機器へ通知

Webブラウザで表示



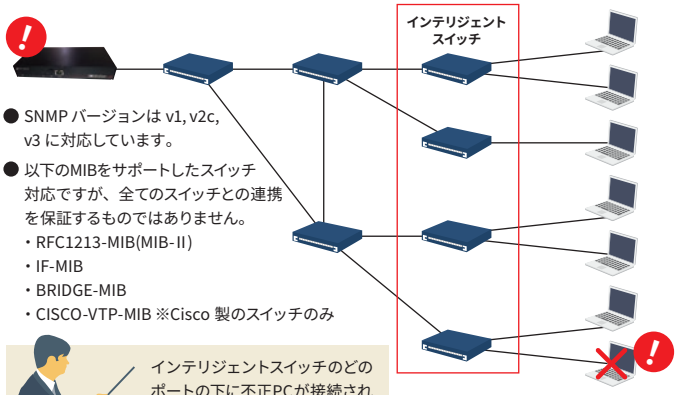
ブロックされた端末のWebブラウザを立ち上げると

❶ ステータス　❷ 利用申請

が表示されます。
お客様の運用に合わせて表示画面及び文言を変更することが可能です。

インテリジェントスイッチ連携

不正機器の接続ポートを把握



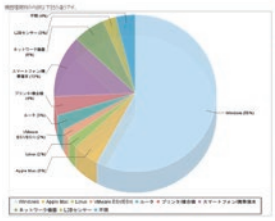
- SNMP バージョンは v1, v2c, v3 に対応しています。
- 以下のMIBをサポートしたスイッチ対応ですが、全てのスイッチとの連携を保証するものではありません。
  - RFC1213-MIB(MIB-II)
  - IF-MIB
  - BRIDGE-MIB
  - CISCO-VTP-MIB ※Cisco 製のスイッチのみ

インテリジェントスイッチのどのポートの下に不正PCが接続されたか場所の特定が可能です。

月次レポート

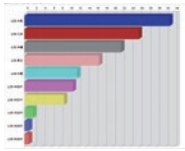
月次レポートを自動作成

【不正端末の検出状況】

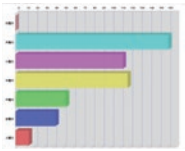


月単位でのレポートを自動的に作成します。
L2Bマネージャー画面上から、レポート出力したい月を指定して、出力できます。
L2Bマネージャーから、個別に検索して頂くことなく全体の管理状況を管理できるので、社内NWつながっている機器の全体把握を簡易的に行なうことが可能です。

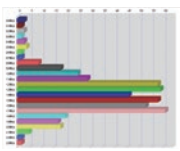
設置場所別



曜日別



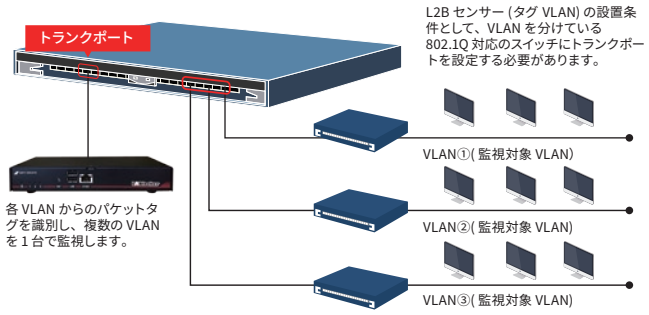
時間帯別



VLAN 環境での利用

L2B センサー (タグ VLAN)

同一拠点内に複数の VLAN が存在する場合、L2B センサー (タグ VLAN) を利用することで 1 台で最大 32VLAN※を監視できます。



※L2B センサー (タグ VLAN)1 台で監視する VLAN 内にある MAC アドレス合計数が 10,000MAC アドレス未満であること

通知機能

以下の内容を管理者へメールで通知
①不正アクセスのブロック
②IP アドレスの変更（DHCP は除く）
③セグメントの移動
④機器名の変更
⑤センサーの異常検知
⑥通信の保留　　等

※メール送信認証は POP-before-SMTP、SMTP-Auth、SMTP over SSL に対応
※syslog サーバへの送信も可能
※SNMP トラップに対応

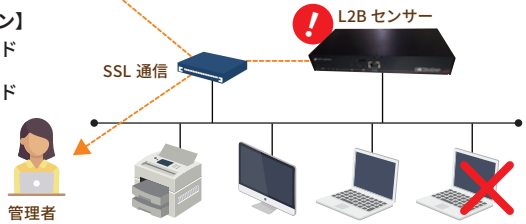
L2Blocker クラウドサービス

L2Blocker のマネージャーをクラウドサービスとして提供

cloud L2Blocker

❶マネージャー用サーバ不要
❷センサーの購入不要
❸必要な期間だけ利用※最低利用期間あり

【選べるプラン】
- スタンダード
- プリペイド
- ハイブリッド



※L2B センサーはレンタルで提供いたします
※サービス詳細は別紙「サービス仕様書」及び「利用規約」をご確認下さい

連携ソリューション

サイバー攻撃対策

ネットワーク監視センサー

Deep Discovery™ Inspector

通信パケットを収集し、相関分析から内部脅威を可視化。マルウェアの感染によるリスク拡大を最小化します。

ネットワークセキュリティアプライアンス

Firebox

マルウェアに感染した端末の通信をゲートウェイで止めるだけでなく、感染した端末自体を緊急遮断し、二次感染等の被害拡大リスクを低減します。

次世代ファイアウォール

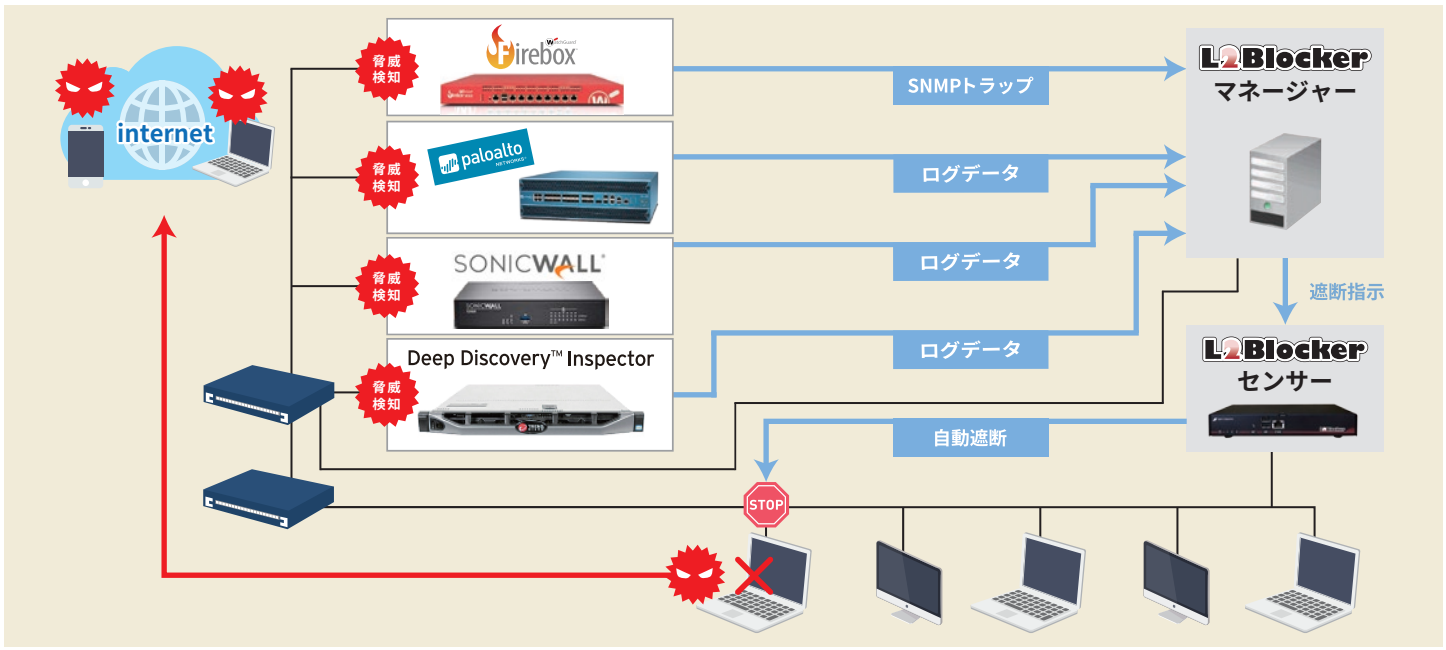
paloalto NETWORKS

次世代ファイアウォールで感染疑義のある通信を検知し、検知ログを L2Blocker に送信し、即時遮断。マルウェアの内部感染拡大のリスクを低減し、被害を最小化します。

次世代ファイアウォール

SONICWALL

次世代ファイアウォールと L2Blocker の連携は、マルウェア感染の初期段階で自動対処することにより内部感染拡大を防止し被害の最小化を図ることができます。



※連携する製品が端末の IP アドレスを特定できる環境であることが前提条件です。

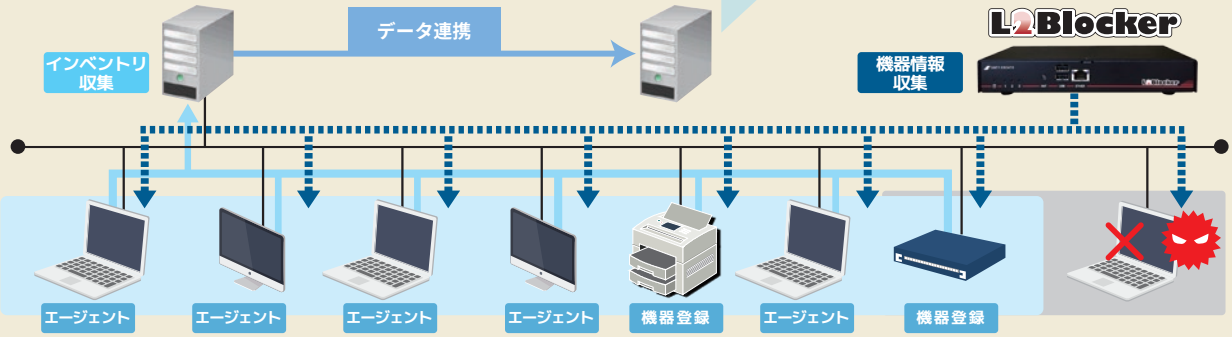
エンドポイントセキュリティ対策

IT 資産管理システム

IT 資産管理システムの管理用エージェントソフトがインストールされていない端末を検知し、是正を促し、IT 資産管理による管理を徹底します。

LANSCOPE Endpoint Manager
SKYSEA Client View
AssetView
System Support best1
ISM CloudOne
eSurvey+
QND Advance Standard

是正対象端末の検知に留まらず、リスクと判断する場合は、L2Blocker で強制遮断を自動で実施することも可能です。



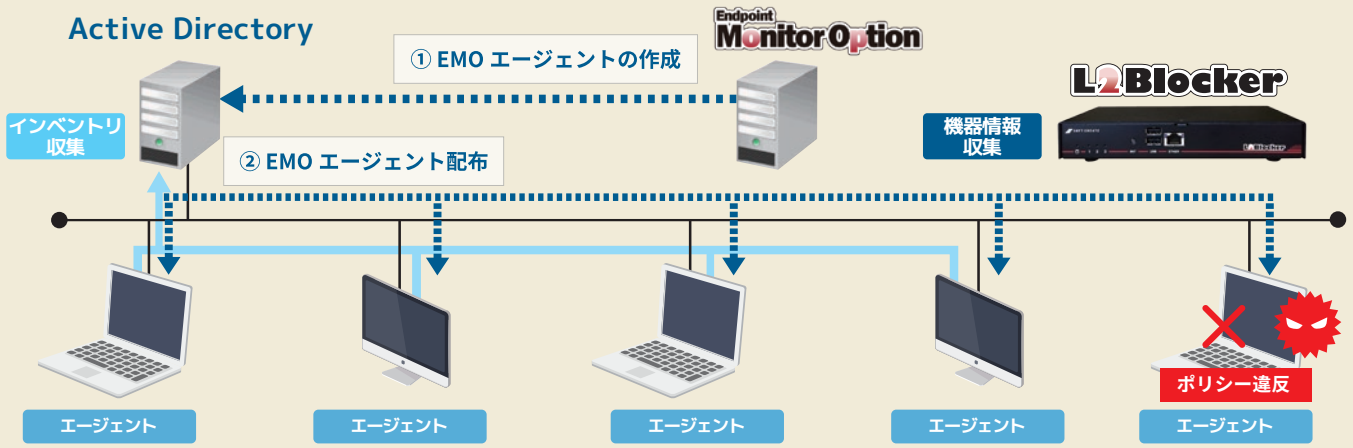
セキュリティポリシーチェック
(オプション)

Endpoint Monitor Option

L2Blockerで許可されている Windows 端末に対して ポリシー適用状況を監視

❶社内ポリシー違反を検知・遮断

エージェントがインストールされた管理 PC からハードウェア、ソフトウェア情報も取得します。エージェントにて収集された情報を L2B マネージャーのホワイトリストに反映することで、より充実した管理台帳として活用頂けます。



【ポリシーチェック】
・ソフト導入チェック・ソフト稼働チェック
・システム構成チェック・レジストリチェック

③ PC 起動時に実行

※配布は、非常駐型のエージェントです。
Active Directory のスタートアップスクリプトでの配布・実行が前提です。

Windows Update 状況や主要ソフトウェアの 脆弱性をチェックしマルウェア対策

❷QFE 最終更新日

Windows Update を実施した最終日をチェックし、更新日が古い端末を自動的に遮断することが可能です。

❸ソフトウェア脆弱性検知

IPA で公開されている脆弱性があるバージョンのソフトウェアを利用している機器をチェックし、脅威レベルによって自動遮断することが可能です。

【対象ソフトウェア】
・Adobe Acrobat Reader
・Adobe Flash Player
・Oracle Java
・Google Chrome
・Mozilla Firefox

※本オプションは、有償です。L2Blocker が別途必要です。
※L2B マネージャー 1 台あたりのエージェント最大管理数は、10,000 台までです。
※エージェント対応 OS は、Windows のみです。

L2Bマネージャー動作環境

CPU	Intel製の2.0GHz 以上（4Core 以上） または同等の互換プロセッサを搭載したコンピューター
メモリ	8GB以上のメモリ
OS	Windows Server 2016（64bit） Windows Server 2019（64bit） Windows Server 2022（64bit） Windows Server 2025(64bit) Windows 10（64bit） Windows 11（64bit） ※日本語のみ、Server Core未対応
ディスク容量	Cドライブに10GB以上の空きが必要
WEBサーバ	Apache Tomcat 9
WEBクライアント	Microsoft Edge、Google Chrome
DB	Microsoft SQL Server 2017/2019/2022 Express Edition
ネットワークポート	オンプレ L2BM通信用：http（TCP：9837）、センサー通信用：（TCP：9827） クラウド L2BM・センサー通信用：https（TCP：443）

※サーバー推奨スペック値は10,000MAC Address/100 セグメント以内かつEndpoint Monitor Optionを同時に利用していないことがご利用の前提です。
※Windows 10（64bit）/ Windows 11（64bit）はL2Bマネージャーの検証を目的とした利用のみ想定しています。ご利用制限：1,000MAC Address/2セグメント以内。

閾値

マネージャー1台あたりのセンサー最大管理数	1,000
マネージャー1台あたりのMACアドレス最大管理数	300,000
センサー1台あたりの監視MACアドレス最大数	10,000
タグVLAN版センサー1台あたりの最大VLAN管理数	32
ネットワーク速度	5Mbps以上を推奨

※管理対象が30,000MAC Address/500セグメント（センサー冗長構成の場合は250）を超える場合は有償版のSQL Serverが必要になります。

製品販売

希望小売価格	L2Bマネージャー	L2M4-311	¥240,000
	L2Bセンサー（スタンダード版）	L2S4-132S	¥140,000
	L2Bセンサー（タグVLAN版）	L2S4-131V	¥340,000
	ラックマウントキット	L2S4-601	¥25,000
年間保守費	初年度の保守は無償サポートとなり次年度より有償です。 次年度以降の保守費は1年契約では製品価格の12%、追加4年一括契約は8%です。		
保守サービスの内容 問い合わせ対応	製品の使用方法に関する問い合わせをE-mailで受付 受付は365日24時間対応 返答はエクスジェン・ネットワークス営業日にて対応		
保守サービスの内容 L2Bマネージャーの保守	マイナーバージョンアップ・リビジョンアップの無償提供 サポートサイトからダウンロードサービスにて提供 ※メジャーバージョンアップは含まれません。		
保守サービスの内容 L2Bセンサーの保守	故障時の代替機の提供 ※故障判定なく、保守申込書に記載された設定を施し、郵送致します。 ※故障時の代替機は新品とは限りません。		

※L2Bセンサーの保守サービス可能期間は購入時から5年間です。
※保守サービスはL2Bマネージャーを含む、保有するL2Bセンサー全台の加入が必須です。

L2Bセンサーのハードウェア仕様

CPU	Intel Atom x5-E3930（動作クロック ベース:1.3GHz）
記憶媒体	メインメモリ 2GByte DDR3L-1866 データ領域 8GByte eMMC（MLC）
LAN	1000Base-T
電源	電源電圧AC100～220V 消費電力：8W（平均）/12W（最大）
電源条件	許容電圧変動：AC100V～220V ±10% 周波数：50～60Hz±3Hz ※付属のACケーブルは100V用になります。
動作環境	周辺温度 0～50°C 周辺湿度 20～90%（結露しないこと）
外形寸法	幅214mm×奥行105mm×高さ37.4mm（ゴム足を含む）
信頼性	EMC VCCI-ClassA適合 IEC61000-4-2（ESD）、Level 2 振動JIS C0040準拠 有害物質 鉛フリー、RoHS10対応

※時刻はL2Bマネージャーとの時刻同期。
※L2Bマネージャーへの接続時にバージョンを自動同期。

構成

L2Bマネージャー	L2Bマネージャーは本システムを稼働させる上で、1つ必要 L2Bマネージャー1に対し、L2Bセンサーがnの構成となる
L2Bセンサー（スタンダード版）	L2Bセンサーはブロードキャストセグメント1つに対して1台必要 ※ARPのパケットを取得している機能となるため、ブロードキャストセグメント毎に1台必要となります。 ※セカンダリセグメントを監視する場合は追加でセンサー1台が必要となります。
L2Bセンサー（タグVLAN版）	タグVLANを構成しているスイッチのトランクポートに接続することにより、32VLANまでを1台のL2Bセンサーで対応可 ※1台のスイッチで33以上のタグVLANを構成している場合には、L2Bセンサーは複数台必要となります。 ※複数台のスイッチで複数のタグVLANを構成している場合には、スイッチ分のL2Bセンサーが必要となります。 ※セカンダリセグメントを監視する場合は追加でセンサー1台が必要となります。

クラウドサービス

初期費用	月額費用の1ヶ月分	
月額利用料	L2Bマネージャー	¥20,000
	L2Bセンサー（スタンダード版）	¥3,000
	L2Bセンサー（タグVLAN版）	¥9,000
サービス利用時間	センサーの稼働時間及びマネージャーの利用できる時間は 24時間365日（ただし計画停止は除きます） 問い合わせ対応などはエクスジェン・ネットワークス営業日	
最大通信速度	1Gbps（ベストエフォート） ※共有回線です	
セキュリティ	httpsによる暗号化通信 L2Bマネージャー環境にはファイアーウォールを設置 データ通信時ウィルスチェック L2Bマネージャーへの接続はIPアドレス限定の設定	
サービス内容	問い合わせ対応、システム監視、システムバックアップ、 システムのバージョンアップ、センサー設定及び貸出、 センサー故障時の交換、月次レポート、 システム障害対応など	

※クラウドサービスL2Bマネージャーの価格は、MACアドレス数が10,000MAC以下、セグメント数が500セグメント以下の価格です。管理数を超過する場合は別途ご相談ください。

詳しくはWEBへ https://www.l2blocker.com/

ご注意
- 本製品を正しく安全にご使用頂くため「取扱説明書」をよくお読みください。
- 本製品を、人身に直接かかわる安全性を要求されるシステムに適用する可能性がある場合には、事前にご相談ください

［開発元］

EXGEN NETWORKS
USE INNOVATIVE TECHNOLOGY.

エクスジェン・ネットワークス株式会社

〒101–0052 東京都千代田区神田小川町1–11 千代田小川町クロスタ11F
TEL 03–3518–8055 FAX 03–3518–8056 E-mail idminfo@exgen.co.jp
https://www.exgen.co.jp/

［お問い合わせ先］