

ニューノーマル時代のセキュリティ対策

「オフィスワーク×テレワーク」のハイブリッド勤務 にオススメのシンプルセキュリティ

エムオーテックス株式会社



新しい働き方に応じたセキュリティ対策とは

ハイブリッド勤務に対応するための注意点

企業に「新しい働き方」の波

2019年4月1日より施行された「働き方改革関連法」を皮切りにテレワークのニーズが高まる中、今回の新型コロナウイルスによって導入が加速。テレワークを採用する企業が増えています。テレワークは交通障害時などの出勤できない場合にも有効（事業継続性＝BCP）であることから、政府や自治体がその実施を推進しています。

tele + work = telework
(離れた) (働く) (会社から離れた場所で働く)

ICTを活用し
場所や時間にとらわれない働き方



国や自治体が補助金・助成金制度でテレワークの整備を支援

テレワーク支援の状況：テレワーク設備の導入に活用できる補助金・助成金制度

支援として、様々な補助金・助成金制度が用意されています。例えば国が支援している『IT導入補助金』『時間外労働等改善助成金（テレワークコース）』や、自治体などが実施している「事業継続緊急対策（テレワーク）事業」などがあり、テレワーク導入に当たって設備投資を検討される企業様はぜひ一度、利用できる支援制度が無いかご確認ください。

IT導入補助金

主幹組織：経済産業省

制度概要

中小企業を対象に、生産性向上に寄与するIT投資に対して補助。

新型コロナウイルスの感染拡大対策として、テレワーク整備などに取り組む事業者を優先的に支援するため、特別枠（C類型）を創設。

補助金額

補助額の上限：30～450万円

補助率：1/2 **（特別枠は2/3）**

働き方改革推進支援助成金（テレワークコース）

主幹組織：厚生労働省

制度概要

テレワーク実施のために必要な設備導入やコンサルティング、就業規則・労使協定等の作成・変更にかかる費用を補助。

2020年5月に、支給上限額の陪乗が発表され、支給の条件も緩和。

補助金額

補助額の上限：300万円

補助率：3/4（目標未達の場合は1/2）

事業継続緊急対策（テレワーク）事業

主幹組織：東京都

制度概要

東京都内に本社を構える中堅・中小企業に対し、テレワークの導入に必要な機器やソフトウェア等の経費を補助。

補助率が10/10と、他の制度に比べて高いことが特徴。

補助金額

補助額の上限：250万円

補助率：10/10

※2020年5月時点の情報のため最新情報はご確認ください

厚生労働省の「働き方改革推進支援助成金（テレワークコース）」

テレワークの導入に必要な機器やソフトウェア、クラウドサービスの導入に加え、導入のためのコンサルティング費用や、研修・教育の費用など、テレワークの導入にかかわる様々な費用に幅広く活用できることが大きな特徴です。ポイントは成果目標が2つ設定されていることです。幅広く活用できる制度となっており、申請期限も12月1日までと比較的余裕がある制度です

■ 制度のポイント

- 2つの成果目標が設定され、
達成状況によって補助率と上限額が変動。
- 受け入れている**派遣労働者**がテレワークを行う場合も対象となる。

■ 助成対象となる事業

□	テレワーク用通信機器(※)の導入・運用 (例) ・シンクライアント端末(パソコン等) ・VPN装置 ・web会議用機器 ・社内のパソコンを遠隔操作するための機器、ソフトウェア ・保守サポートの導入 ・クラウドサービスの導入 ・サテライトオフィス等の利用料 など ※ シンクライアント以外のパソコン、タブレット、スマートフォンの購入費用は対象となりません	□ 就業規則・労使協定等の作成・変更 (例) テレワーク勤務に関する規定の整備
		□ 労務管理担当者に対する研修
		□ 労働者に対する研修、周知・啓発
		□ 外部専門家(社会保険労務士など)による導入のためのコンサルティング

■ 2つの「成果目標」と、達成状況に応じた補助率と支給上限額

①	評価期間に1回以上、対象労働者全員に、在宅またはサテライトオフィスにおいて就業するテレワークを実施させる
②	評価期間において、対象労働者が在宅またはサテライトオフィスにおいてテレワークを実施した回数の週間平均を、1回以上とする

成果目標の達成状況	達成	未達成
補助率	3/4	1/2
1人当たりの上限額	40万円	20万円
1企業当たりの上限額	300万円	200万円

出典：厚生労働省「働き方改革推進支援助成金（テレワークコース）」より <https://www.mhlw.go.jp/content/11909000/000622080.pdf>

※2020年5月時点の情報のため最新情報はご確認ください

【参考】支援制度ナビ：COVID-19に関連した助成金、補助金検索サイト

各地方、支援団体による助成金・補助金制度が、まずはお住いの地域で検索してみましょう。

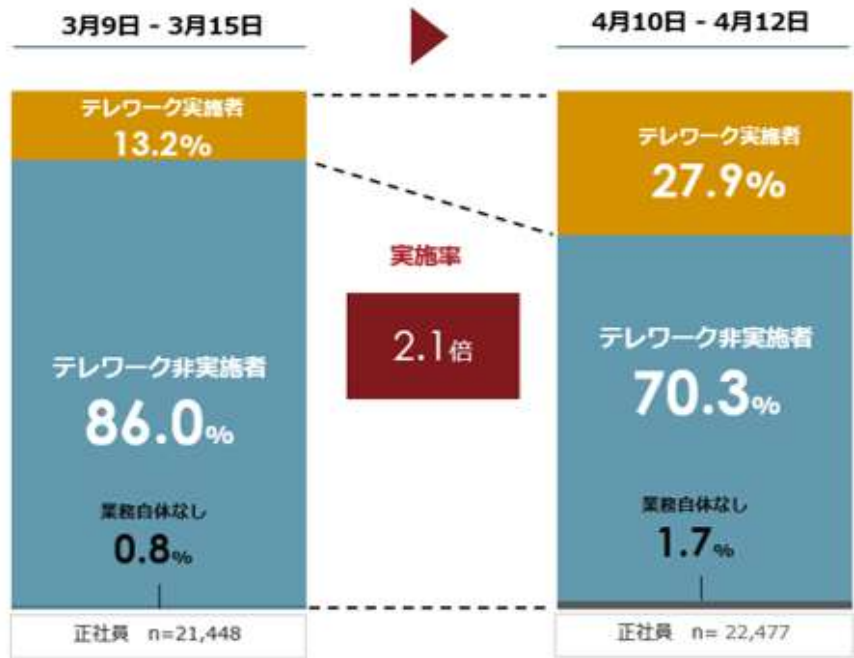


株式会社クラウドシエン 支援制度ナビ <https://covid19.seido-navi.com/>

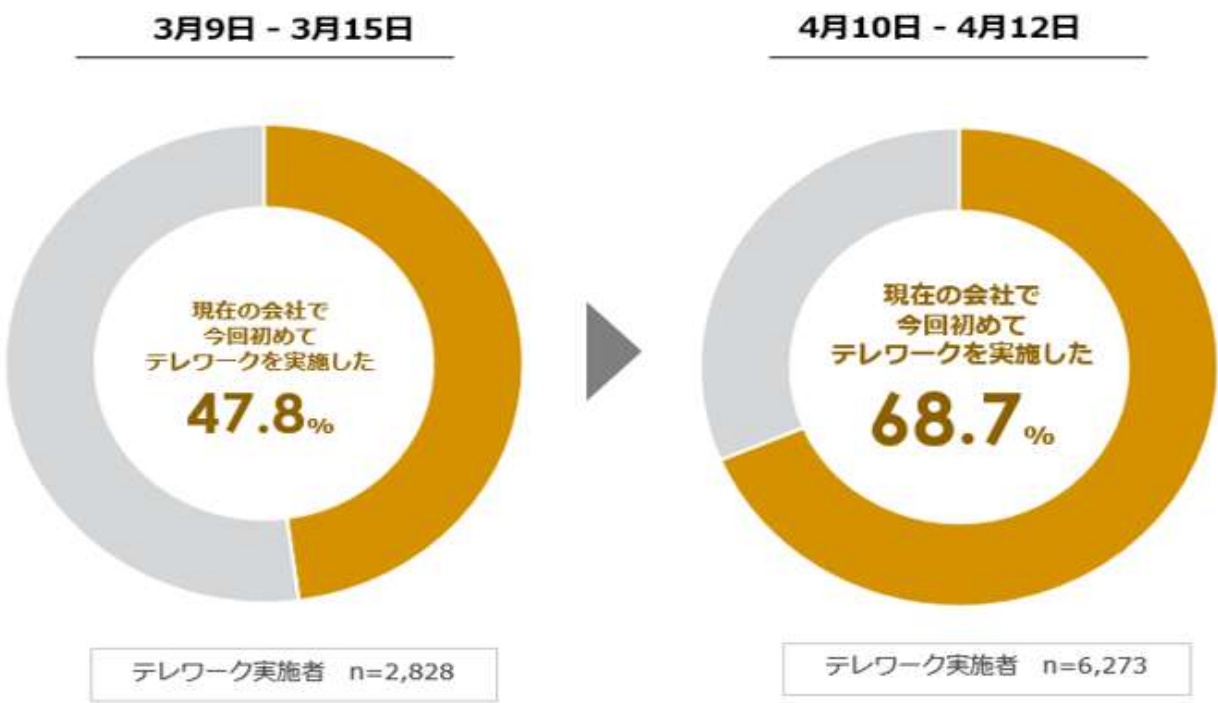
テレワークの実態

テレワーク実施率は全国平均で27.9%。1か月前の13.2%に比べて2倍以上増えています。また約半数が今回初めてテレワークを実施、その数も日を追うごとに増えている状況です。コロナ禍における「働き方」の手段としてテレワークが定着しつつあることが分かります。

図表1. 3月と4月のテレワーク実施率



図表2. 3月と4月の初めてのテレワーク実施率



出典：パーソル総合研究所 <https://rc.persol-group.co.jp/news/202004170001.html>

コロナ後テレワークはようになる？ 実施企業の約半数が継続希望

テレワーク先進国の米国企業であるFacebook社では、今後5～10年をかけて約5万人の従業員の50%を在宅勤務の目標を掲げています。またGoogleが行った日本国内アンケートでは、テレワーク継続に対する方針は、「当面はテレワークを継続」「段階的にオフィス勤務を解禁」「職種によって対応を変える」など企業によって異なる結果となりました。

●テレワーク継続意向



2020年1月以降にテレワークを始めたオフィスワーカーのうち、**今後もテレワーク派は49%、続けたくない派が23%**。オフィス&テレワーク混合で働いている人よりも、完全テレワーク（毎日テレワーク）で働いている人の方が継続意向が強く、社員からも求められる働き方に。

<米国Facebook社の方針>

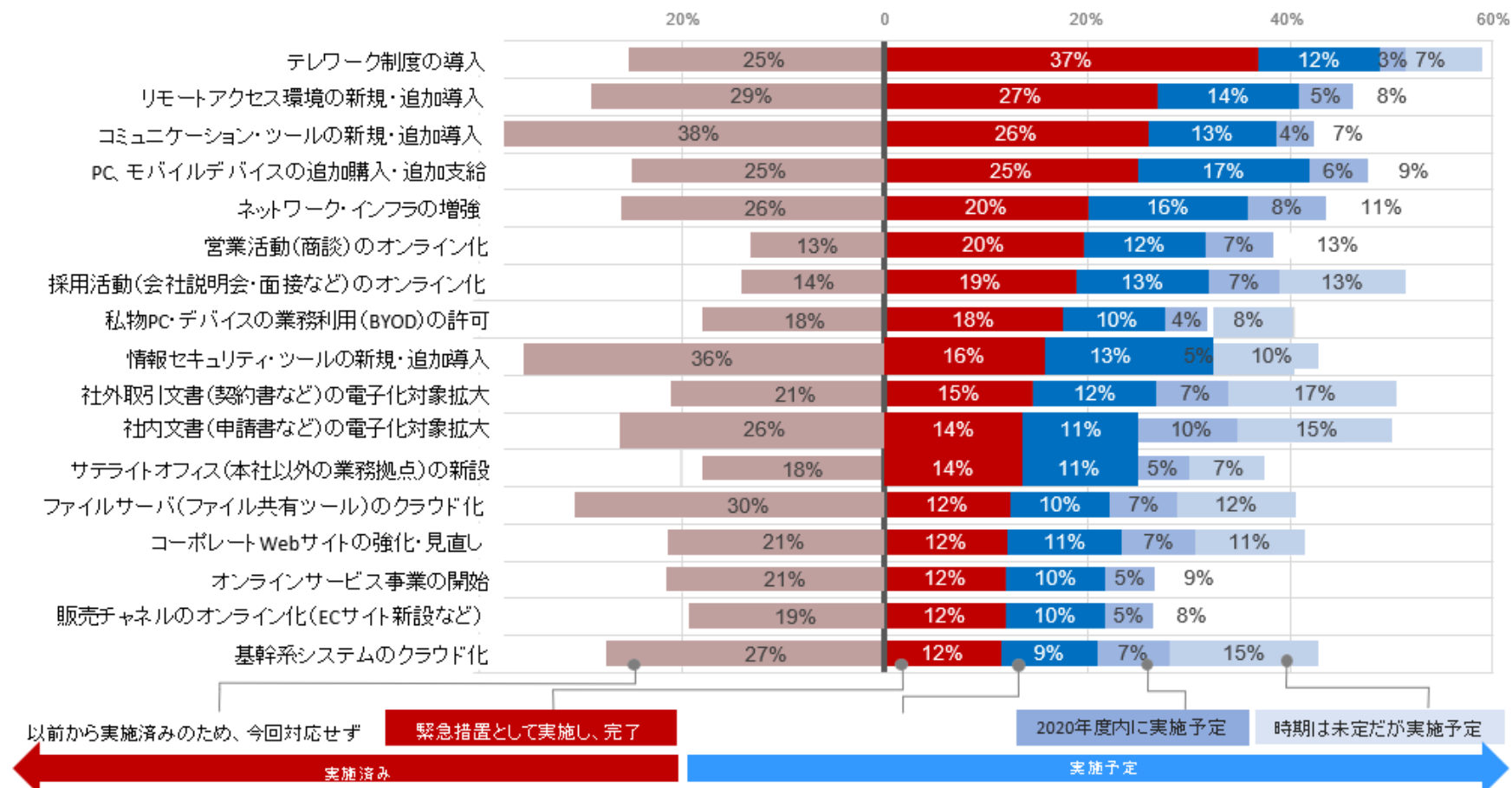


Facebook社内でのアンケートによると、**半数以上が在宅でもオフィスと生産性が変わらない**と答え、**約40%が完全な在宅勤務に関心**を持っている一方、半数以上がなるべく早くオフィスに戻りたいと考えているという。

出典：Think With Google「テレワークを続けたい」のはどんな人？ 3000人に聞いた今・これからの働き方
<https://www.thinkwithgoogle.com/intl/ja-jp/articles/interview/covid-19-8/>

テレワーク実施企業におけるIT投資実態

実際、現場においてもIT投資は伸長しています。2020年4月時点で緊急措置としてツールや機器を中心にテレワーク投資(グラフ：赤)が実施されており、業務を行うために必要な投資が行われたことが分かります。投資自体は今後(青)も継続して投資が続く事が予想され、緊急事態宣言解除後も投資がなされると予想されます。

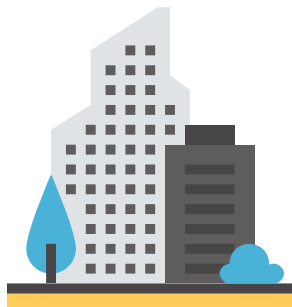


出典：ITR「コロナ禍の企業IT動向に関する影響調査」(2020年4月調査)

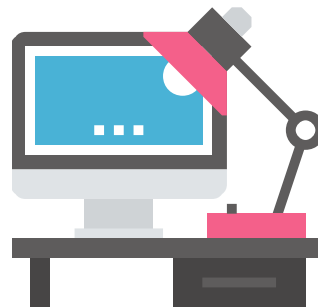
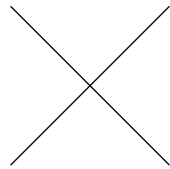
© 2020, ITR Corporation All rights reserved.

多様化する今後の勤務形態

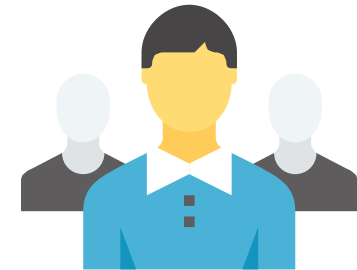
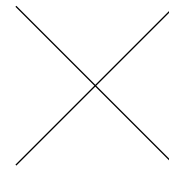
世の中の動向、現場の希望、終わらない感染状況などを踏まえると今後は、従来の「オフィス勤務」メインの働き方から、「テレワーク」や「サテライトオフィス」などが混在したハイブリット勤務が想定されます。緊急事態宣言禍の経験を活かした企業の業務に合わせた「新しい働き方」を中長期的に取り組む必要があります。



オフィスワーク



在宅・テレワーク



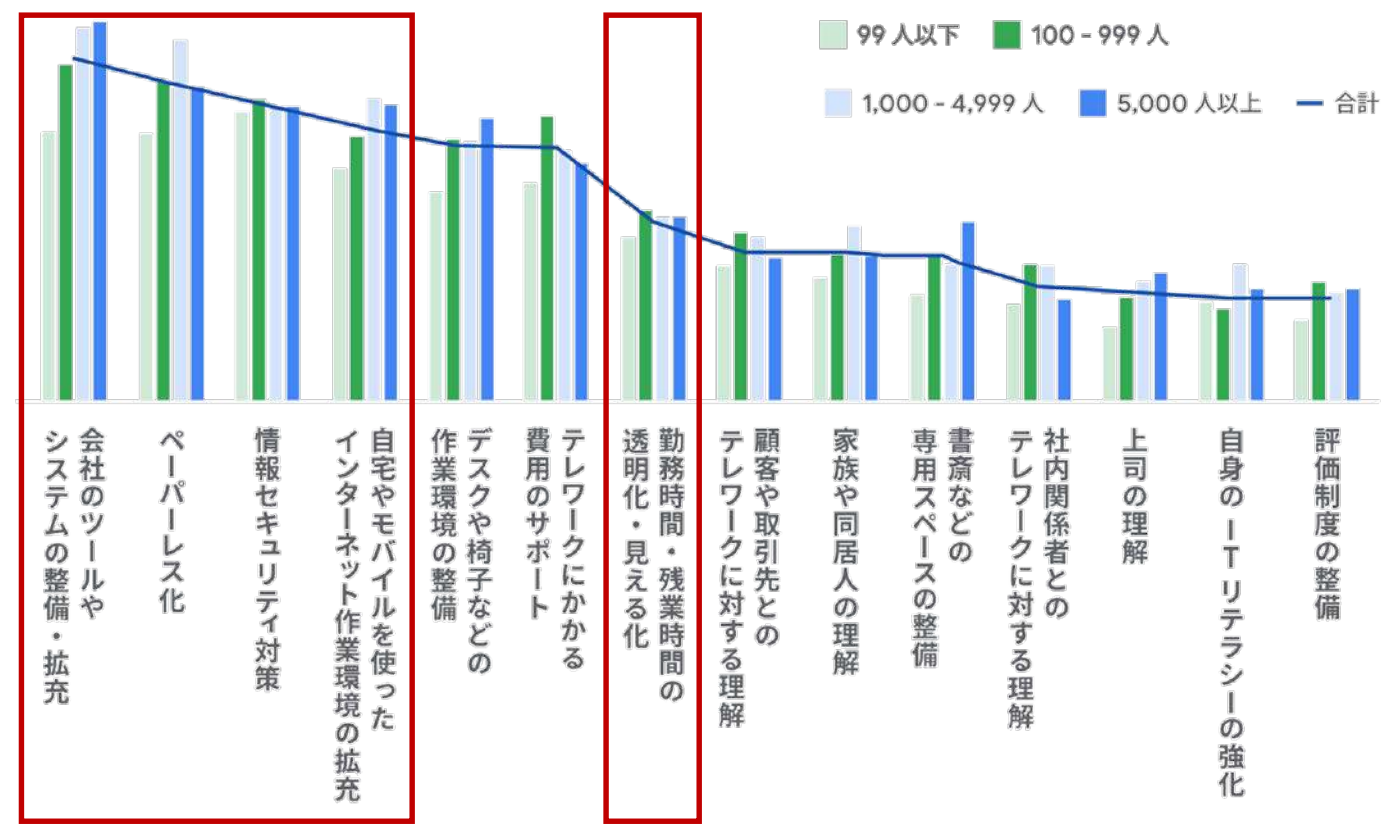
サテライトオフィス等の
共有スペース

withコロナフェーズとして新しい働き方を想定、中長期的に取り組む必要あり

新しい働き方「オフィスワーク×テレワーク」の課題

ハイブリッド勤務に対応するには、課題の洗い出しから始める事が重要です。課題として挙がっているのは「環境整備」「セキュリティ」「見える化」が挙げられます。特にテレワーク未実施企業がテレワークに踏み切れない理由が「見える化」です。IT投資にはこの3要素を満たすことが求めていることが分かります。

●今後テレワークを継続するにあたり、必要だと思うこと



テレワーク実施課題 TOP3

環境整備

見える化

セキュリティ

<テレワーク実施済企業>

実施したは良いが**業務状況が「見えなくなり」不安**

<テレワーク未実施済企業>

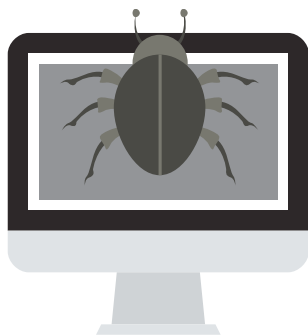
業務状況が「見えなくなる不安」があり踏み切れない

出典：Think With Google今後テレワークを継続するにあたり、必要だと思うこと <https://www.thinkwithgoogle.com/intl/ja-jp/articles/interview/covid-19-11/>
引用：2020年4月8日 東京商工会議所「新型コロナウイルス感染症への対応に関するアンケート」調査結果<https://www.tokyo-cci.or.jp/page.jsp?id=1021764>

対策急務！企業における見えない機器「シャドーIT」が急増中

実は今、管理者が把握できていない機器「シャドーIT」が急増しています。テレワーク対応として緊急的に導入したPCやモバイルデバイス、やむを得ずBYOD運用を認めた企業では、それらの利用把握が難しく、機密情報の取り扱いや有償ソフトウェアの利用も把握できない状態が考えられ、ライセンス違反のリスクやセキュリティホールとなる危険があります。

< 緊急事態宣言解除後に行っておくべきシャドーITリスクチェック >



緊急許可した端末の
利用実態と状況確認



緊急許可した機器における
有償ソフトウェアの状況



BYODの利用状況と
業務利用状況



BYOD利用の
業務関連資料の削除状況

管理者が把握できていない機器＝シャドーITが急増中

シャドーITのリスクとは

シャドーITの放置には様々なリスクがあります。例えば、セキュリティソフトを導入していない私物端末を社内ネットワークに接続してしまうと、会社規模でのマルウェア感染の危険性があります。証拠管理ができていないため追跡調査なども難航します。さらに想定外の利用のためDHCPの枯渇など業務に影響を及ぼすといった事も考えられます。



脆弱性対応・マルウェア対応

脆弱性のあるOS・アプリの利用で
情報搾取やマルウェア侵入の経路に…
攻撃時に防御することも困難



証拠管理

操作ログを監視・記録ができず、
有事の際の証拠が追えない



私的なNW利用(NW遅延・DHCP枯渇)

アプリダウンロードや動画再生により
NWの遅延やDHCPの枯渇が発生する可能性
業務影響を及ぼす

オフィス×テレワークのハイブリッド環境を守る

シャドーITを接続させない究極シンプルなセキュリティ対策

シャドーITの不正接続防止は「L2Blocker」にお任せ！

不正な機器の接続を検知、遮断するアプライアンス製品で、今回のような管理外のシャドーIT機器の接続を検知すると、自動で遮断をしてくれます。そもそも管理外の機器の接続をさせないのでインシデント自体を未然に防ぐことができるため、初期対応としてのセキュリティ対策におすすめです。



不正接続防止ツール市場 累計導入数No.1※

L2Blocker

- IT資産管理・内部不正対策・外部脅威対策がワンストップで対応可能
- アプライアンスだから既存LAN環境を変えず手軽に始められる
- 24時間365日監視が可能！管理工数を大幅削減
- センドバック・バージョンアップテクニカルサポート付

インベントリ情報収集

不正接続検知

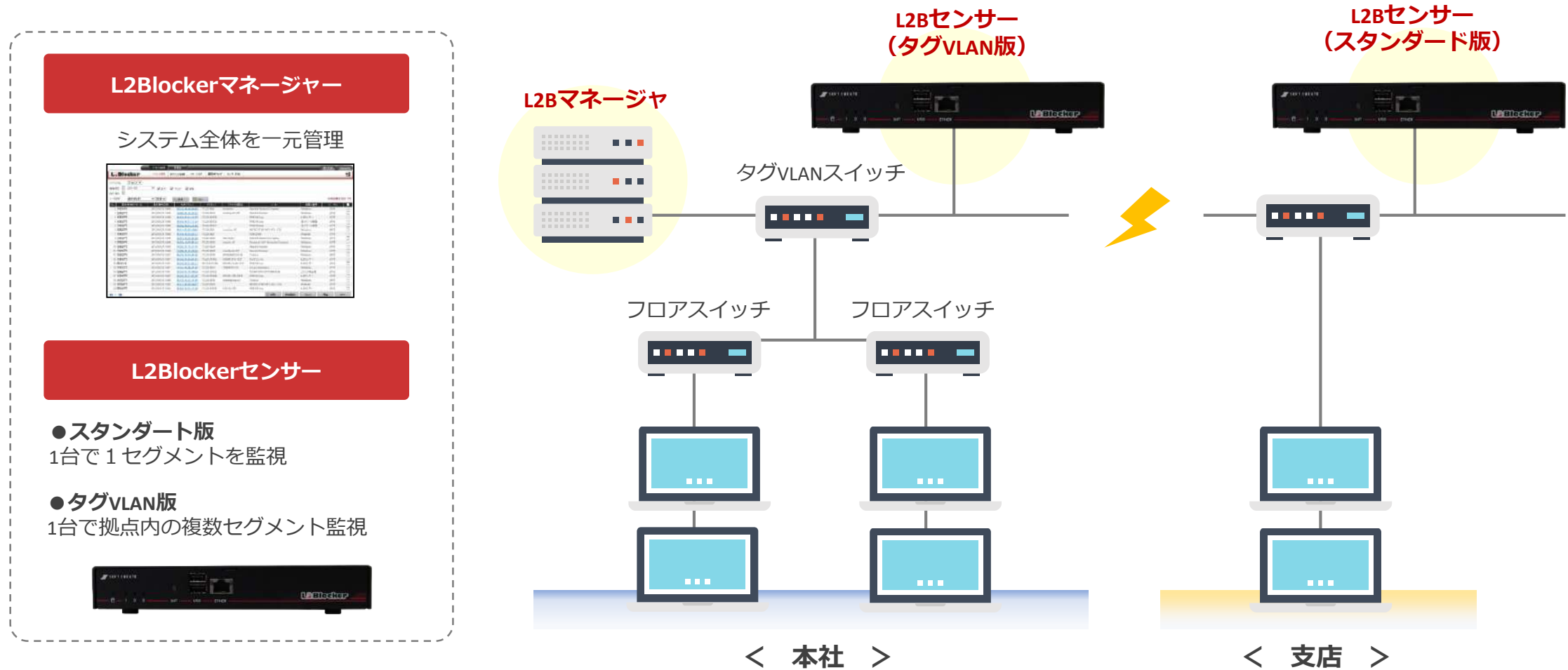
不正接続遮断

<https://www.l2blocker.com/>

※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」

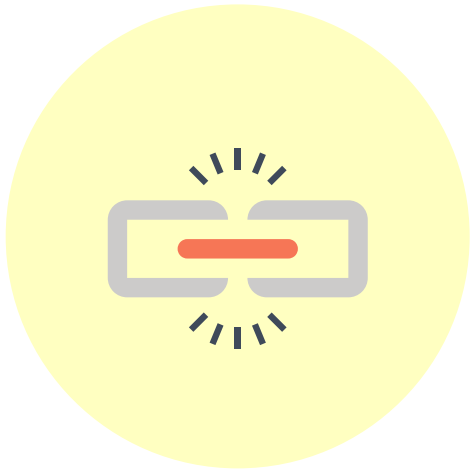
製品構成

管理するための「マネージャー」と監視したいセグメントに「センサー」を導入します。アプライアンスにLANを指すだけなので、今のNW環境をかえず導入が可能です。センサーは2種類あり、スタンダード版で1セグメント分、タグVLAN版ですと1つで最大32セグメント分も監視が可能です



L2Blokerのポイント

専用アプライアンスであるため、24時間365日監視できるので時間と場所を気にせずリスクある接続から守ることが可能です。アプライアンス自体も高い耐久性を持っており、粉じんや熱など過酷な状況である工場にも多く採用されています。またタグVLAN版は1台で最大32セグメント管理が可能のため、業界トップクラスのコスパを誇ります。



接続機器の検知・遮断

アプライアンスにLANを
指すだけで接続機器の検知
情報収集・遮断



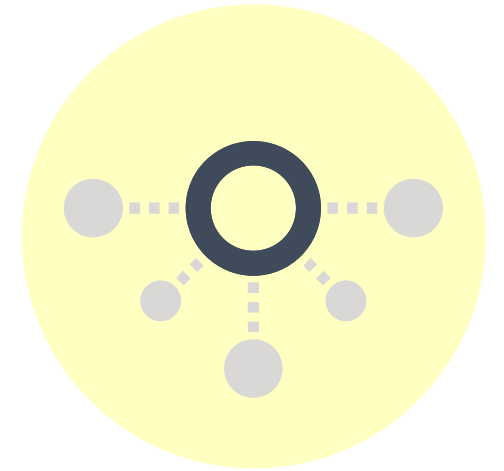
24時間365日監視

アプライアンスなので
電源ON/OFFの心配も不要



高い耐久性

過酷な環境である工場
暑くなるサーバー室でも
安心の耐久性



大規模も安心のコスパ

1台で最大32セグメント！
業界トップクラスの
コストメリット

こんな課題をお持ちの方に最適！

1. 大規模ネットワーク環境における遮断ソリューションの導入
2. 24時間365日安定して監視したい
3. ソフトウェア検知を利用しておりインストールする機器の管理が困っている
4. シャドーITに対するセキュリティ対策が不安

導入フェーズによって選べる3つの動作モードを用意

L2Blockerの機能は「検知」と「遮断」とシンプルですので、運用時も管理の負担も非常に少なく手離れが良い製品です。行いたいセキュリティレベルに合わせた運用を行うことが可能です。
検知・遮断を行う際は、段階的運用を実施する事をおすすめします。

ステップ1	ステップ2	ステップ3
収集モード 初期導入フェーズ	保留モード 初期稼働 or 運用フェーズ	ブロックモード 運用フェーズ
 データを収集するだけでブロックを行わないモードです。<u>初期導入時の許可端末台帳作成</u>に便利な機能です。	 不正端末からのアクセスを即ブロックするのではなく、<u>一定期間許可することができるモード</u>です。 ※ 運用上ブロックできない環境にも有効です。	 L2Blocker本来の機能「<u>不正アクセスをブロックする</u>」モードです。

「検知」社内NWへの接続状況の可視化

「検知機能」としては、様々な種類の機器の検知を行います。仕組みとしては、ARPリクエストによりゲートウェイを確認しており、リクエストを受けたゲートウェイが返信、センサーが情報を探索しリクエストを出さない機器も検知します。

SOFT CREATE

アクセス制限

管理者

個人設定

Password

L2Blocker

アクセス機器

ポリシー制御

アラートログ

画面操作ログ

センサー設定

MR稼働状況

マイクエリ名

デフォルト

検索項目

ステータス

ブロック

保留

条件追加

ソート設定

最終検知日

降順

検索

CSV

検索結果は 105件 です

No	最終検知センサー名	最終検知日時	MACアドレス	IPアドレス	アクセス機器名	メーカー	機器の種類	ステータス	
1	L2B-本社5F	2014/07/09 23:55	7C:C5:37:34:B3:88	192.168	suzuki-no-iPhone	Apple	iPad/iPhone	許可	
2	L2B-九州	2014/07/09 20:19	00:23:6C:50:9D:09	192.168	yamada-no-iPhone	Apple	iPad/iPhone	許可	
3	L2B-本社6F	2014/07/09 19:47	F0:B4:79:E5:B5:F0	192.168	iPad Touch	Apple	iPad/iPhone	許可	
4	L2B-本社6F	2014/07/09 19:38	0C:2B:61:C1:B3:00	192.168	iPhone	Apple	iPad/iPhone	許可	
5	L2B-大阪	2014/07/09 17:06	00:1B:83:F2:7F:2E	192.168	AppleAirMAC	Apple	Apple Mac	許可	

取得可能情報				
MACアドレス	IPアドレス	メーカー名	コンピュータ名	機種の種類
機器の種類				
パソコン・サーバー	ルータ	携帯端末（スマホ）	IP電話	ネットワーク機器

※機器情報の自動取得機能は、全ての機器の機器名取得や機器種別判別を保証するものではありません。

「遮断」 不許可デバイスのネットワーク接続を遮断

不正に接続したデバイスを検知するとブロック（遮断）し、双方に通知が可能です。ARPリクエストによりゲートウェイを確認し、センサーが受信したリクエストを不正接続と判定した場合、ブロック packets を返信しブロックする仕組みです。接続者にも警告通知を出すことが可能で、利用申請フォームの表示も可能なのでIT資産登録のフロー化にも活用できます。

The screenshot shows the L2Blocker management interface. At the top, there's a navigation bar with tabs like 'アクセス制限', '管理者', '個人設定', and 'Password'. Below this, there's a sub-navigation bar with 'アクセス機器', 'ポリシー制御', 'アラートログ', '画面操作ログ', 'センサー設定', and 'MR稼働状況'. The main area has search filters for 'マイクエリ名' (Default), '検索項目' (ステータス), and checkboxes for '許可', 'ブロック', and '保留'. A table lists detected devices with columns: No, 最終検知センサー名, 最終検知日時, MACアドレス, IPアドレス, アクセス機器名, メーカー, 機器の種類, ステータス, and a checkbox. One device is listed: 1, L28-本社7F, 2014/07/09 12:12, [MAC], [IP], koron-01, Buffalo, ネットワーク機器, ブロック. A red box highlights the 'ステータス' and 'ブロック' buttons in the top right.

No	最終検知センサー名	最終検知日時	MACアドレス	IPアドレス	アクセス機器名	メーカー	機器の種類	ステータス	
1	L28-本社7F	2014/07/09 12:12	[MAC]	[IP]	koron-01	Buffalo	ネットワーク機器	ブロック	☐

クライアント側通知

未登録機器の接続をネットワークに接続した場合、ブロックした端末側にも通知が可能です。通知画面は、**通常のお知らせ以外にも利用申請フォーム**も利用可能です。※表示条件あり



【参考】センサーのモードと登録機器のステータス

登録機器のステータス



- 許可** : ネットワーク利用を許可します。
- 保留** : 猶予期間、利用可能期間の設定が可能で、設定期間が経過すると自動的にステータスがブロックとなりネットワーク利用が出来なくなります。
- ブロック** : ネットワーク利用が出来ません。センサーにより通信をブロックします。

センサーの動作モード



- 収集** : 検知された機器全てステータス許可で自動登録されます。
- 保留** : 未登録機器を検知してもステータス保留で登録しブロックをしません。保留期間を設定すれば検知時に自動で猶予期間がステータスに追加されます。
- ブロック** : 未登録及びステータスブロックの機器を検知した際に通信をブロックします。

機器ステータス \ センサーモード	センサーモード		
	MACアドレス収集	保留	ブロック
許可	☐ 通信可	☐ 通信可	☐ 通信可
保留	☐ 通信可	☐ 通信可	☐ 通信可
ブロック	☐ 通信可	☒ ブロック	☒ ブロック

優先ポリシー設定・自動削除機能

L2BlokerではIPアドレスやメーカーコードによる許可・ブロックも可能です。IPアドレスを許可登録しておけば機器の交換時の再設定が不要です。

●IPアドレス・メーカーコードによる許可/ブロックの設定

SOFT CREATE

アクセス制限

管理者

L2Bloker

アクセス機器

ポリシー制御

アラートログ

画面操作ログ

センサー設定

マイクログラム

デフォルト

検索項目

ポリシーの適用

☒有効

☐無効

条件追加

+

ソート設定

優先順位

月曜

検索

CSV

No	管理コード	優先順位	制約ポリシー	ポリシーの適用	IPアドレス制御			メーカー制御	
					指定方法	IPアドレス(FROM)	IPアドレス(To)	指定方法	フィルタ文字列
1	00000006	10	許可	有効	ON(個別)	192.168.105.1		OFF	
2	00000006	11	許可	有効	ON(個別)	192.168.115.1		OFF	
3	00000001	20	許可	有効	ON(範囲)	192.168.105.100	192.168.105.120	OFF	
4	00000002	21	許可	有効	ON(個別)	192.168.105.150		OFF	
5	00000003	100	許可	有効	OFF			ON(コード)	00000029
6	00000004	101							
7	00000005	200							
8	00000007	9999							

IPアドレス制御

指定方法	IPアドレス(FROM)	IPアドレス(To)
ON(個別)	192.168.105.1	
ON(個別)	192.168.115.1	
ON(範囲)	192.168.105.100	192.168.105.120
ON(個別)	192.168.105.150	
OFF		
OFF		
OFF		
OFF		

ルーターやサーバーのIPアドレスによる許可登録することで、故障交換等でMACアドレスが変更された場合でもブロック対象になりません。ポリシー制御レコードは合計5,000レコードまで可能です

●MACアドレス自動削除

L2Bloker

アクセス機器

IPアドレス制御

アラートログ

画面操作ログ

センサー設定

マイクログラム

デフォルト

検索項目

ステータス

☒許可

☒ブロック

☒保留

条件追加

+

ソート設定

最終検知日

降順

検索

CSV

No	最終検知センサー名	最終検知日時	MACアドレス	IPアドレス	アクセス機器名	メーカー	機器の種類	ステータス
1	第1部	2013/03/21 16:08	00:22:04:44:06:00	72.20.58.5	kmishiba	Hewlett-Packard Company	Windows	許可
2	第2部	2013/03/21 16:08	24:0E:05:12:22:FF	72.20.58.33	mskiguchi-HP	Hewlett-Packard	Windows	許可
3	第3部	2013/03/21 16:08	00:06:45:01:10:FB	72.20.58.153		PINON Corp.	128センサー	許可
4	第4部	2013/03/21 16:08	00:06:45:01:10:2A	72.20.58.152		PINON Corp.	ネットワーク機器	許可
5	第5部	2013/03/21 16:08	00:06:45:01:10:67	72.20.58.151		PINON Corp.	ネットワーク機器	許可
6	第6部	2013/03/21 16:08	00:21:05:0F:10:65	72.20.58.9	suemitsu-PC	MICRO-STAR INT'L CO., LTD.	Windows	許可
7	第7部	2013/03/21 16:08	00:15:53:08:0C:12	72.20.58.154				許可
8	第8部	2013/03/21 16:08	2C:41:30:27:02:FB	72.20.58.155				許可
9	第9部	2013/03/21 16:08	70:60:12:0F:55:01	72.20.58.156				許可
10	第10部	2013/03/21 16:08	00:05:05:10:20:68	72.20.58.157				許可

最終検知日時	MACアドレス
2015/06/01 23:55	7C:C5:37:34:B3:86
2015/06/01 23:27	D8:A2:5E:73:3E:DB
2015/06/01 20:19	00:23:6C:50:9D:09
2015/06/01 19:47	F0:B4:79:E5:B5:E0
2015/06/01 19:38	DC:2B:61:C1:B3:00
2015/06/01 17:06	00:1B:63:F2:7F:2E
2015/06/01 16:22	10:93:E9:57:DF:BD
2015/06/01 13:41	00:01:F4:6B:F3:85

設定した期間内で一度も通信を行っていない機器を自動的に登録から削除することが可能、不要リストの増加防止に繋がります。期間設定は、最小1日から最大5年間で設定可能です。

センサー冗長化機能

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）と稼働状況の確認が行えます。 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。

●IPアドレス・メーカーコードによる許可/ブロックの設定

SOFT CREATE

アクセス制限

管理者

L2Blocker

アクセス機器

ポリシー制御

アラートログ

画面操作ログ

センサー設定

MR稼働状況

マイクエリ名

項目幅調整

検索項目

-選択-

条件追加

+

ソート設定

ホスト名

昇順

検索

CSV

ホスト名1つに対してMACアドレスが2つ表示
バックアップ機はグレー表示

No.	ホスト名	VLAN_ID	MACアドレス	IPアドレス	バージョン	センサー名	設置場所(ネットワーク)	動作モード	稼働状況	
1	softcreate-01	0010	00:0A:85:04:03:C1	192.168.10.100	4.4.1	L2B-本社5F	開発部門 (192.168.10.XXX)	保留	○	
			00:0A:85:04:03:D1	192.168.10.102	4.4.1				○	
2	softcreate-02	0020	00:0A:85:04:03:C2	192.168.20.100	4.4.1	L2B-本社6F	営業部門 (192.168.20.XXX)	ブロック	○	
			00:0A:85:04:03:D2	192.168.20.102	4.4.1				○	
3	softcreate-03	0030	00:0A:85:04:03:C3	192.168.30.100	4.4.1	L2B-本社7F	ネットワーク部門 (192.168.30.XXX)	MACアドレス収集	○	
			00:0A:85:04:03:D3	192.168.30.102	4.4.1				○	
4	softcreate-51	0000	00:0A:85:04:03:C4	192.168.200.100	4.4.1	L2B-大阪	大阪支社 (192.168.200.XXX)	保留	○	
5	softcreate-61	0000	00:0A:85:04:03:C5	192.168.210.100	4.4.1	L2B-東北	東北支社 (192.168.210.XXX)	ブロック	○	
6	softcreate-71	0000	00:0A:85:04:03:C6	192.168.220.100	4.4.1	L2B-九州	九州支社 (192.168.220.XXX)	MACアドレス収集	○	

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

スイッチ連携機能

L2Blockerを監視対象としているセグメント内のインテリジェントスイッチと連携させる事で、不正接続をブロックした際に、どのスイッチのどのポートに接続されたのか判別が可能です。配置場所と備考を活用すれば、すぐに場所を特定が可能です。

●スイッチ連携

SOFT CREATE

L2Blocker

アクセス制限

監視スイッチ

管理者

スイッチ・ポート

スイッチ連携

SNMP設定

EPM Option

マイクエリ名

デフォルト

検索項目

-

-選択-

条件追加

+

ソート設定

スイッチ名

昇順

検索

CSV

No	スイッチ名	IPアドレス	SNMP設定名	情報収集日時	機器の説明	機器の名称	ポート数				設置場所	備考
							all	up	down	test		
1	L2-Cisco	172.20.59.130	デフォルト 設定(v3)	2015/09/17 19:58	Cisco C3750E Software, Version 15.0(2)SE5	SW-CS-L2-PS3	30	1	29	0	本社-4F-PS3	プロダクト&サービス部
2	L2-アライドテレシス	172.20.59.52	デフォルト 設定(v3)	2015/09/17 19:58	Allied Telesis router/switch, AW+ v5.4.4-3.5	SW-AT-L2-PS1	9	6	3	0	本社-4F-PS1	プロダクト&サービス部
3	L2-エレコム	172.20.59.56	デフォルト 設定	2015/09/17 19:58	EHB-SG2A08-PL 10x1G Ethernet Switch	SW-EL-L2-PS2	10	1	9	0	本社-4F-PS2	プロダクト&サービス部
4	L2-バッファロー	172.20.59.54	デフォルト 設定	2015/09/17 19:58	BUFFALO BS-GS2008P	SW-BF-L2-PS4	8	1	7	0	本社-4F-PS4	プロダクト&サービス部

スイッチ情報を収集

アラートログ

前回検出時から情報の変更があった場合、アラートログへ記録され検索も可能です。管理者への通知は内容ごとに受け取り設定が可能です。アラートの通知は、メールもしくはSNMPトラップにて送信することができ、アラートの項目毎に受信設定が行えますので運用に合わせて項目を選択ください。

SOFT CREATE

L2Blocker

アクセス制限

管理者

スイッチ連携

EPM Option

アクセス機器

IP・メーカー制御

アラートログ

画面操作ログ

センサー設定

MR稼働状況

マイクエリ名

項目幅調整

検索項目

アラート内容

ブロック

IPアドレスの変更

セグメントの移動

機器名の変更

WebAPI登録

条件追加

ソート設定

検知日時

降順

検索

CSV

No	検知日時	MACアドレス	IPアドレス	検知センサー名	アラート内容	備考
1	2017/06/01 23:02:10	00:00:EB:41:82:8E	192.168.20.252	L2B-本社6F	機器名の変更	demo-pc ⇒ nichikaw
2	2017/06/01 23:02:10	00:00:74:70:41:0D	192.168.30.19	L2B-本社7F	IPアドレスの変更	192.168.10.254 ⇒ 192.168.30.19
3	2017/06/01 23:02:10	00:00:74:70:41:0D	192.168.30.19	L2B-本社7F	セグメントの移動	L2B-大阪 ⇒ L2B-本社7F
4	2017/06/01 22:02:10	00:00:F4:5E:3D:6F	192.168.20.150	L2B-本社6F	機器名の変更	demo-pc ⇒ hoomori3
5	2017/06/01 22:02:10	00:00:74:75:EF:A4	192.168.30.4	L2B-本社7F	IPアドレスの変更	192.168.10.254 ⇒ 192.168.30.4
6	2017/06/01 22:02:10	00:00:74:75:EF:A4	192.168.30.4	L2B-本社7F	セグメントの移動	L2B-大阪 ⇒ L2B-本社7F
7	2017/06/01 21:02:10	00:00:74:90:8E:8F	192.168.30.21	L2B-本社7F	IPアドレスの変更	192.168.10.254 ⇒ 192.168.30.21
8	2017/06/01 21:02:10	00:00:74:90:8E:8F	192.168.30.21	L2B-本社7F	セグメントの移動	L2B-大阪 ⇒ L2B-本社7F
9	2017/06/01 21:02:10	00:00:F8:D8:1A:A1	192.168.30.65	L2B-本社7F	機器名の変更	demo-pc ⇒ kshino
10	2017/06/01 20:02:10	00:00:EB:41:82:8E	192.168.20.252	L2B-本社6F	IPアドレスの変更	192.168.10.254 ⇒ 192.168.20.252
11	2017/06/01 20:02:10	00:00:EB:41:82:8E	192.168.20.252	L2B-本社6F	セグメントの移動	L2B-大阪 ⇒ L2B-本社6F

アラート通知

利用申請 (送信可否) *

● 送信しない ● 送信する

利用申請 (メール件名)

[L2BM]ネットワーク利用申請

接続保留 (送信可否) *

● 送信しない ● 送信する

接続保留 (メール件名)

[L2BM]接続保留 通知メール

接続ブロック (送信可否) *

● 送信しない ● 送信する

接続ブロック (メール件名)

[L2BM]接続ブロック 通知メール

センサー障害 (送信可否) *

● 送信しない ● 送信する

センサー障害 (メール件名)

[L2BM]L2Blocker障害 通知メール

IPアドレス変更 (送信可否) *

● 送信しない ● 送信する

IPアドレス変更 (メール件名)

[L2BM]IPアドレス変更 通知メール

セグメント移動 (送信可否) *

● 送信しない ● 送信する

セグメント移動 (メール件名)

[L2BM]セグメント移動 通知メール

機器名変更 (送信可否) *

● 送信しない ● 送信する

機器名変更 (メール件名)

[L2BM]機器名変更 通知メール

レポート作成 (送信可否) *

● 送信しない ● 送信する

レポート作成 (メール件名)

[L2BM]レポート作成 通知メール

ポリシー違反 (送信可否) *

● 送信しない ● 送信する

ポリシー違反 (メール件名)

[L2BM]ポリシー違反 通知メール

システム障害 (送信可否) *

● 送信しない ● 送信する

システム障害 (メール件名)

[L2BM]システム障害 通知メール

L2Blocker×LanScope Cat連携

L2BlockerはIT資産管理ツールと親和性が高くLanScope Catとも連携が可能です。連携することで企業のIT資産管理の効率化が可能です。

不正接続防止ツール市場 累計導入数No.1※

業界トップシェアの統合型エンドポイントマネジメント



LanScope Catが入っていれば自動的に接続許可し、LanScope Catが入っていない場合、L2Blockerが自動で切断

LanScope Cat未導入の場合、機器へ直接警告通知。Catのインストールを促し、的確に管理下に配置



※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 × LanScope Catで実現するネットワークの可視化と正常化のステップ

1. 組織内のネットワーク機器の情報をもれなく収集

L2Blocker

設置したセンサーがネットワーク機器のインベントリ情報を自動収集。ネットワーク接続機器をもれなく把握

2. 不許可デバイスのネットワーク接続を遮断

L2Blocker

管理済の機器をホワイトリストに登録。管理外の不許可デバイスのネットワーク接続を遮断

3. 管理外のネットワーク機器が存在しないかチェック

L2Blocker × LanScope Cat

L2Blockerで検出したネットワーク機器が、LanScope Catで管理済みかを管理画面で確認。未申請機器をチェック

4. Cat導入済み機器はホワイトリスト登録不要

L2Blocker × LanScope Cat

管理下端末はホワイトリスト登録なしで接続を許可。新規PC購入時の作業工数を大幅削減

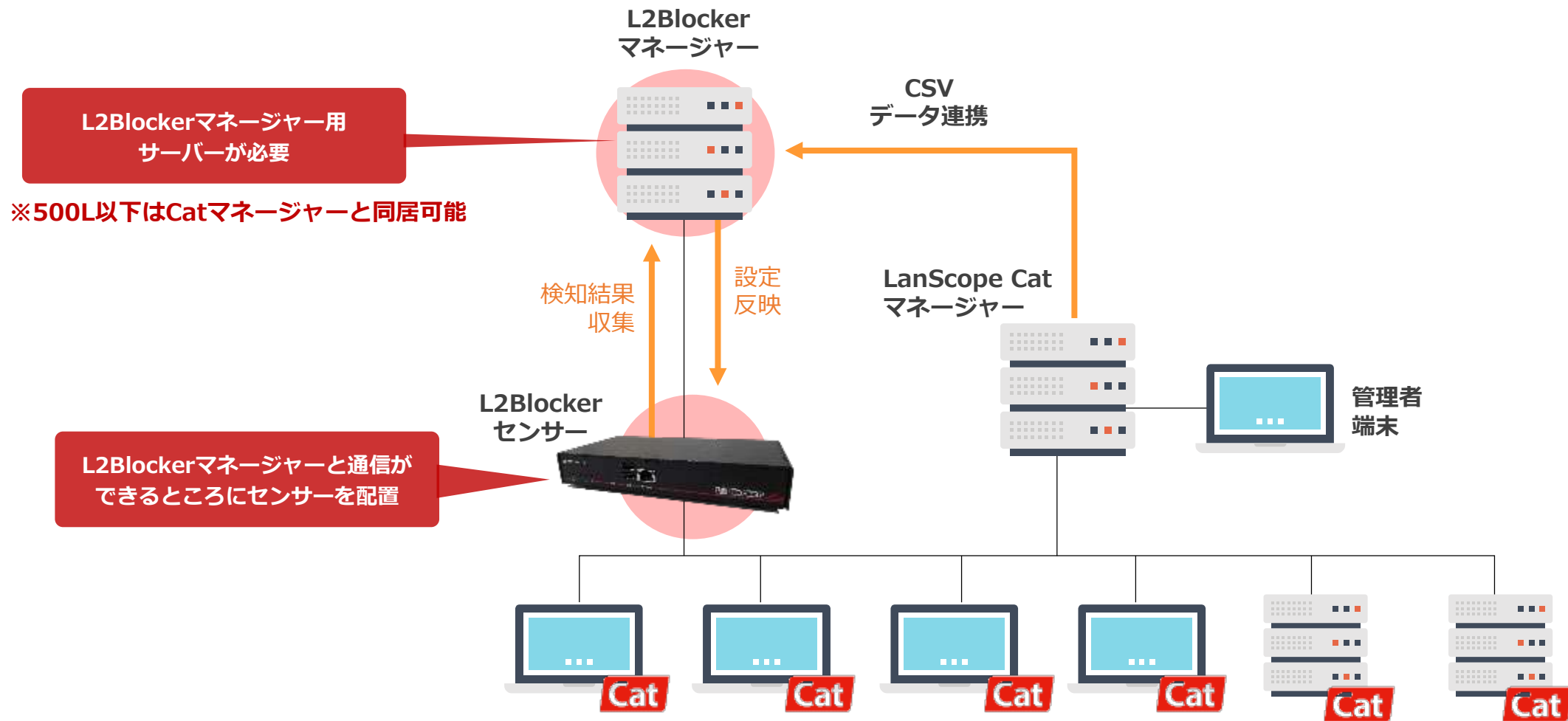
4. 遮断された機器に対してCatのインストールを誘導

L2Blocker × LanScope Cat

ネットワークから遮断されたPCにCatインストールを促すメッセージ配信。新規購入PCへ登録作業を簡素化

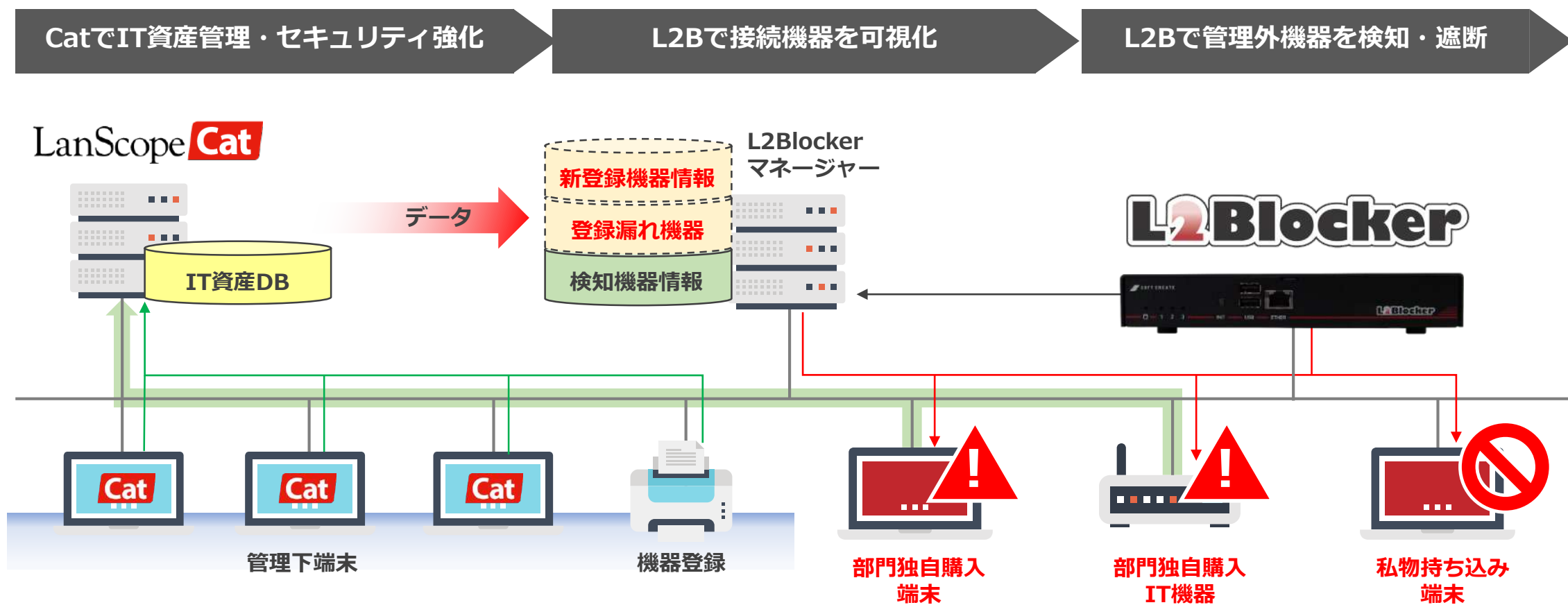
L2Blocker×LanScope Catのシステム構成図

連携する場合は、L2Blocker用のサーバーの設置に加えて、センサーはL2Bマネージャーと通信ができる場所に設置します。管理台数が500Lまでであれば、LanScope CatのサーバーとL2Blockerサーバーは同居が可能です。



L2BlockerとLanScope Catとの運用イメージ

Cat導入済機器は自動的に接続は許可され、Cat未導入機器は企業ポリシーに合わせて段階的に運用フローを回せます。警告を出し是正を行うにとどめる運用や、自動的に遮断を行う事もできます。加えて遮断を行った上で、L2Blockerから警告画面を利用しCatのインストールを促すという流れも可能ですので、Catの管理下に置くための働きかけの手段としても活用可能です。



管理外のネットワーク機器が存在しないかチェック

LanScope Catで管理済の機器の情報をL2Blockerに連携することで、管理済みの機器かも確認も簡単に出来ます。

SOFT CREATE

アクセス制御

管理者

スワイチ連携

EPM Option

個人設定

Password

L2Blocker

アクセス機器

IP-メーカー制御

アラートログ

画面操作ログ

センサー設定

MR稼働状況

マイクエリア名

IT資産(幅調整)

特殊条件

☐ MACアドレスを機器ごとに集約して表示する

検索項目

選択

条件追加

ソート設定

検索

CSV

どこで

いつ

どんな機器が接続されたか

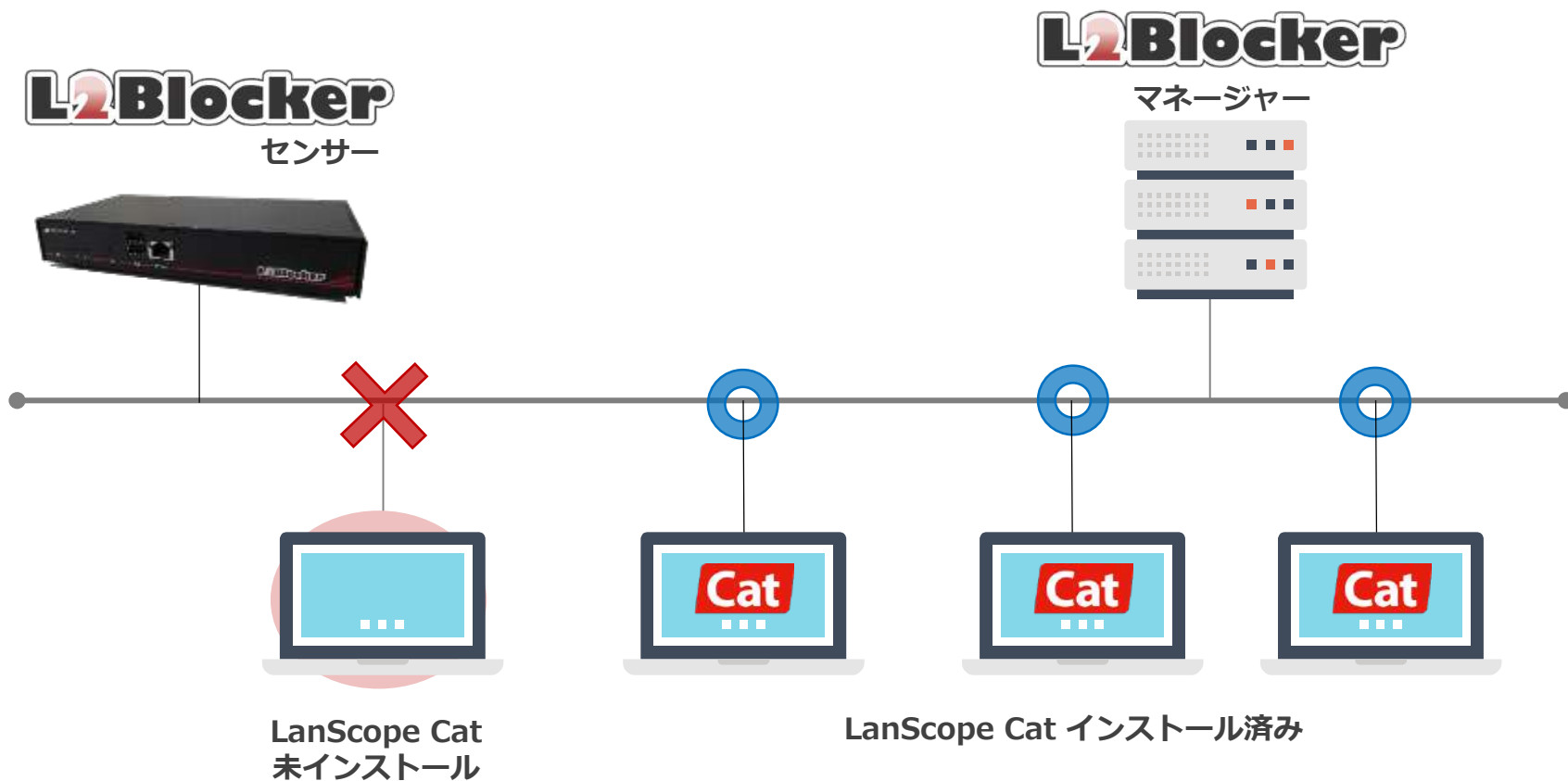
LanScope Catで管理済の場合は「連携済み」に「○」が表示される

No	最終検知センサー名	最終検知日時	MACアドレス	IPアドレス	アクセス機器名	機器の種類	製造元/メーカー	IT資産管理システム連携				ステータス	
								エージェント	情報収集日	連携済	管理対象		
1	プロダクト&サービス部	2016/08/19 15:43	00:0C:29:0F:27:F0	10.60.76.4	vm-skysea	Windows 2008	VMware	○	2016/08/19	○	管理する	許可	☐
2	プロダクト&サービス部	2016/08/19 15:43	00:08:A5:61:80:0F	10.60.76.3	L2B-V4-HONBAN	L2Bセンサー	PINON Corp.	-		×		許可	☐
3	プロダクト&サービス部	2016/08/19 15:43	00:1A:50:92:F3:F5	10.60.76.2	L2-Switch	ネットワーク機器	Allied Telesis	-		○		許可	☐
4	プロダクト&サービス部	2016/08/19 15:43	00:0C:29:0B:4C:82	10.60.76.5	vm-test-pc	Windows 7	VMware	○	2016/08/17	○	管理する	許可	☐
5	プロダクト&サービス部	2016/08/19 15:42	60:72:5C:1A:E0:DE	10.60.76.1	L3-Switch	ルータ	Cisco Systems	-		○		許可	☐
6	プロダクト&サービス部	2016/08/19 15:41	20:08:EB:66:4A:4E	10.60.76.6	tuematsu-n2	Windows 10	Panasonic	×		×	管理する	許可	☐



Cat導入済み機器はホワイトリスト登録不要

LanScope Catインストール済みの機器が接続されると自動で許可しますので、別途L2Blokerでのホワイトリスト登録は不要で、運用工数の削減が可能です。



Catインストール済みのPCは許可登録なしで接続が可能

遮断された機器に対してLanScope Catのインストールを誘導

遮断PCに対してメッセージを表示を表示できるので、新規購入PCへのLanScope Catの展開を簡便化することが可能です。



画面印刷

★★★ネットワーク管理者からのお知らせ★★★

この機器のネットワーク接続は許可されていません。
Windowsの場合は、[ここ](#)からセットアップファイルをダウンロードしてインストールし、パソコンを再起動してください。
それ以外の機器を利用している場合は、ネットワーク管理者にご連絡ください。

接続機器情報

MACアドレス:	00:0C:29:CA:DD:8A
IPアドレス:	172.20.58.12

LanScope Catのクライアントプログラムのインストールを促すメッセージを表示

※管理者が許可したくない端末にもMRインストールさせられるため、運用には注意が必要。専用ポートの利用を推奨します
※反映のタイミングはCatのCSV出力とL2Bインポートのタスクスケジューラー設定の時間

不正接続防止だけじゃない！サイバー攻撃時代に対応したL2Blockerの機能もご用意

不正機器の排除



セキュリティ対策ソフトのインストール状況や利用を禁止しているソフトウェアの利用を監視し、セキュリティリスクが高いと判断される端末を自動的に遮断することが可能です。

https://www.l2blocker.com/endpoint_monitor

リスク端末の排除



次世代FW「Paloalto」で検知したマルウェア感染疑義端末をL2Blockerが即時自動遮断を行います。

<https://www.l2blocker.com/paloalto>

リスク端末の排除



DDIより出力されたログ情報から脅威レベルが高い外部へのC&CserverへのコールバックのみL2Blockerで自動遮断を行います。

<https://www.l2blocker.com/ddi>

ご購入について

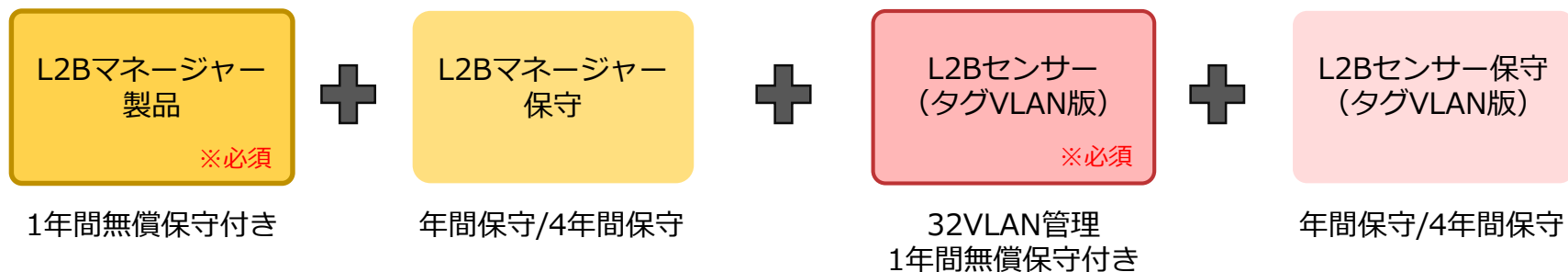
仕様・スペック・価格

L2Blockerの購入方法

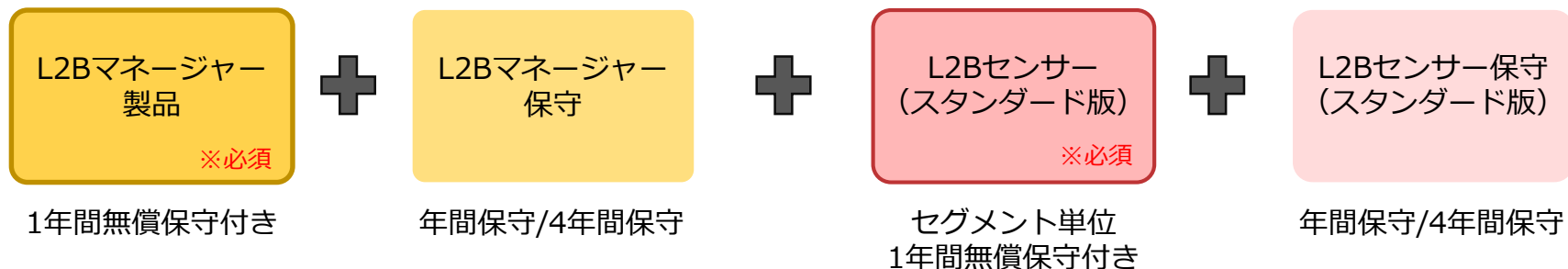
マネージャー必須で、規模やネットワーク構成によって2種類の機器から選択導入

最大10万MACアドレス・1,000セグメントの管理が可能。VLAN/セグメントの数に応じてセンサーの購入が必要です。

●大規模/本社管理構成（初年度58万～）

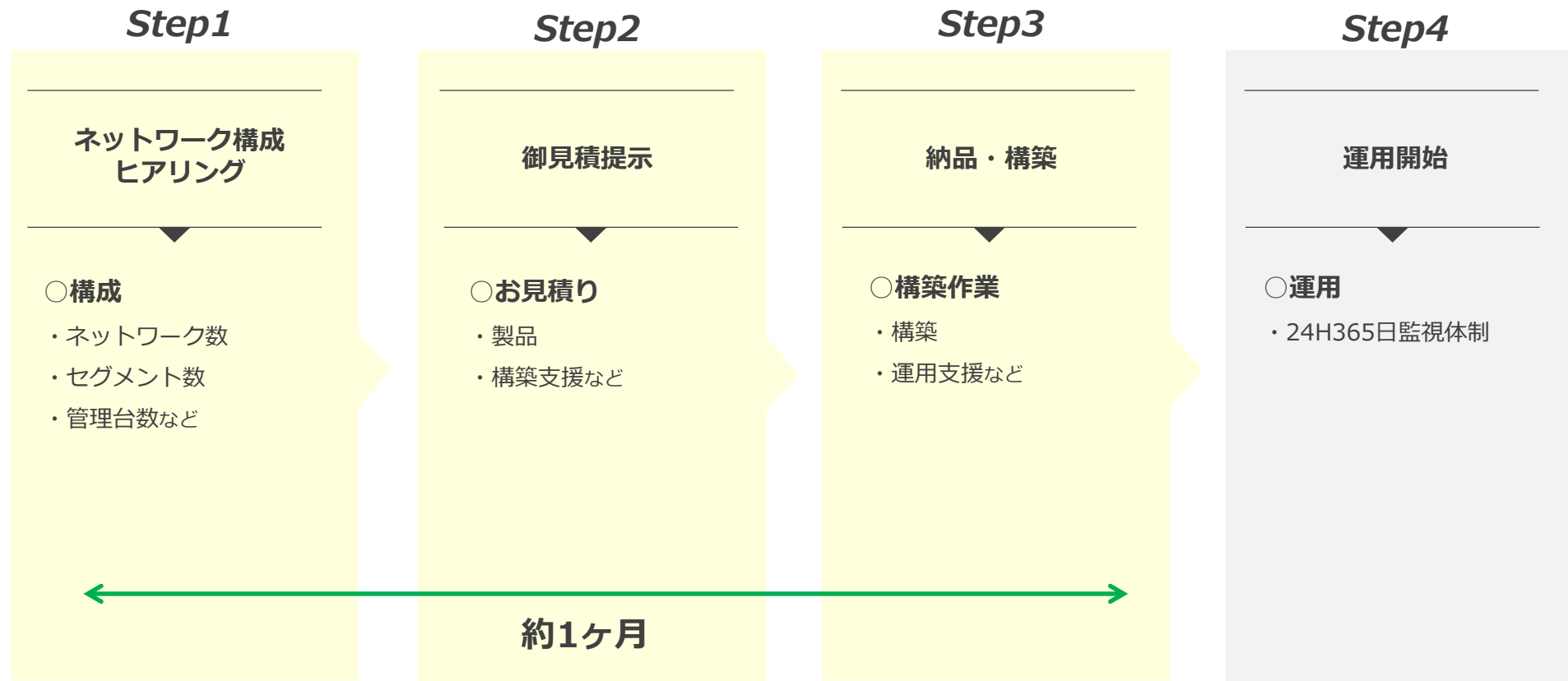


●小規模/拠点管理構成（初年度38万～）



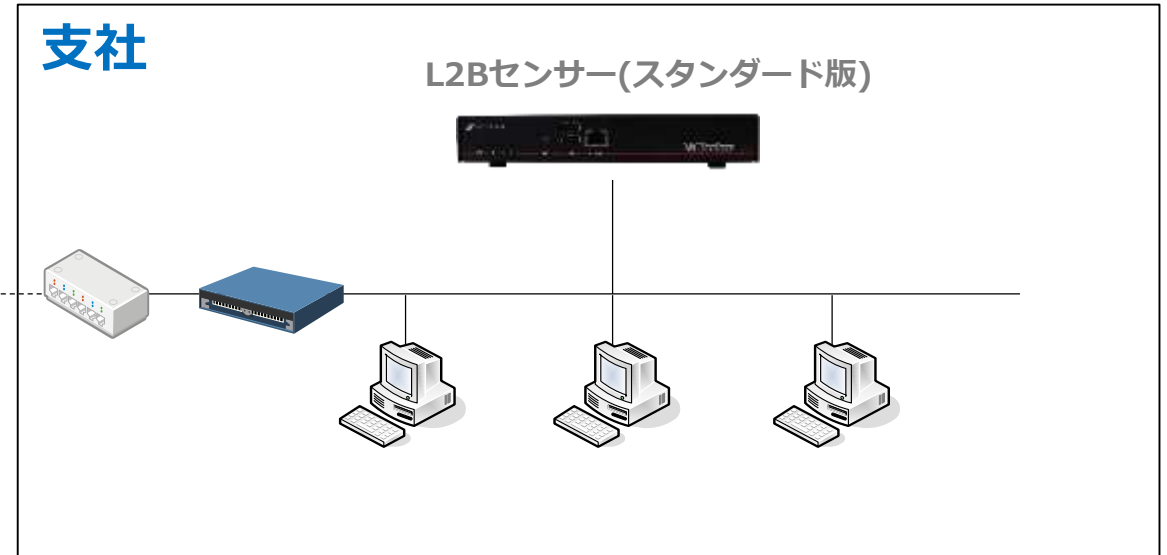
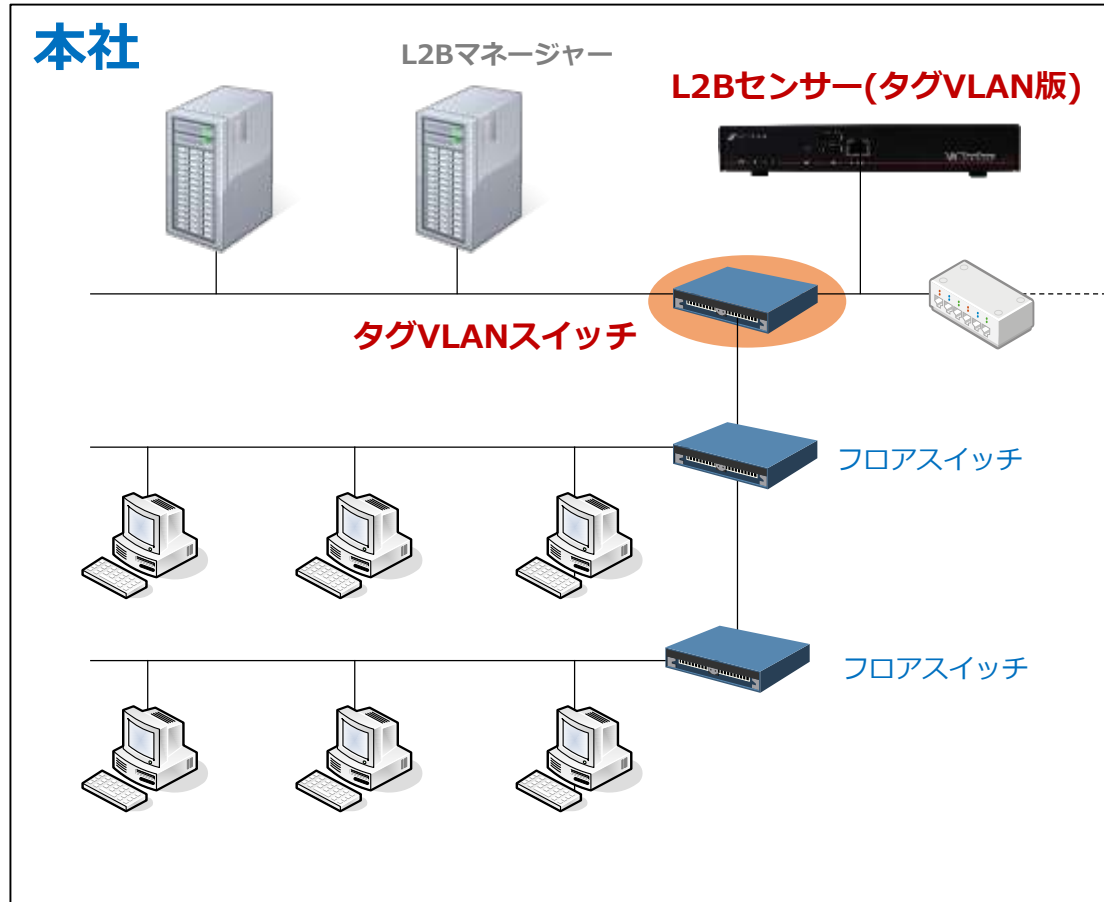
L2Blockerの検討～導入のステップ

お客様のご要望・ネットワーク構成に合わせてご提案いたします



※お客様の要件によって期間は変動します

【補足】 L2Blockerの購入方法（タグVLAN版センサーの利用イメージ）



- 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**すると、32VLANまでを1台のセンサーで対応可
- 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数分のセンサーが必要

タグVLAN版センサーで管理できるのは同一のタグVLANスイッチで管理するネットワーク（＝**1拠点内**）の複数セグメント

L2Blocker動作環境

● LanScope Cat 不正接続防止ツール L2BlockerマネージャーVer.4

	1,000 MAC Address 10セグメント環境	10,000 MAC Address 100セグメント環境	30,000 MAC Address 500セグメント環境	100,000 MAC Address 1,000セグメント環境
CPU	Intel 製CPU 2.0GHz 以上 (2Core 以上)	Intel製CPU 2.4GHz 以上 (2Core以上)	Intel製CPU 3.0GHz 以上 (4Core以上)	Intel製CPU 3.0GHz 以上 (4Core以上)
メモリ	6GB 以上	8GB 以上	10GB 以上	12GB 以上

※MACアドレスが30,000件か500セグメント(冗長構成の場合250セグメント)以上を管理する場合は有償版のSQL Serverが必要

● L2Bマネージャーディスク消費サイズ

	1,000 MAC Address 10セグメント環境
プログラム領域 (SQL Server)	約6GByte
プログラム領域 (マネージャー)	1GByte
データ領域	最大20GByte
ログ領域	目安として 20KB × MAC Address数

※ログ領域は1日あたりの消費量 ※ログの保持期間はデフォルトで30日間

●通信データ

下記環境を想定した場合、センサーとマネージャー間で、更新時に約150KBのデータ通信が発生します。

- ・管理MACアドレス：30,000件
1セグメント辺りの機器数：3,000台

●ネットワーク速度

1セグメントあたり512kbps以上を推奨

※上記の値は更新時間5分、管理MACアドレス30,000件を想定した推奨値となります。

LanScope Cat×L2Blocker同居時のスペックと推奨環境

2019年11月29日更新

●推奨スペック

LanScope Cat管理端末台数	L2Blocker監視対象	LanScope Cat 統合マネージャー兼サブマネージャー + L2Blocker マネージャー	
100台	MACアドレス：300 セグメント数：10	CPU	2.6GHz以上
		メモリ	8GB
		HDD容量	500GB以上
		使用DB	SQL Server Express Edition※
500台	MACアドレス：1500 セグメント数：30	CPU	2.6GHz以上
		メモリ	8GB
		HDD容量	1.7TB以上
		使用DB	SQL Server Express Edition※

※データベースは、「SQL Server 2012」「SQL Server 2017」に対応しています。

●対応OS

OS名	Edition	動作確認済Service Pack	Cat統合マネージャー	Catサブマネージャー	L2Blockerマネージャー
Windows Server 2016	Standard	なし	9.0.0.0～	9.0.0.0～	4.7.4～
	Datacenter	なし	9.0.0.0～	9.0.0.0～	4.7.4～
Windows Server 2012 R2	Standard	なし	9.0.0.0～	9.0.0.0～	4.7.4～
	Datacenter	なし	9.0.0.0～	9.0.0.0～	4.7.4～
Windows Server 2012	Essentials	なし	9.0.0.0～	9.0.0.0～	4.7.4～
	Standard	なし	9.0.0.0～	9.0.0.0～	4.7.4～
	Datacenter	なし	9.0.0.0～	9.0.0.0～	4.7.4～
Windows Server 2008 R2	Standard (×64)	なし／SP1	9.0.0.0～	9.0.0.0～	4.7.4～
	Essentials (×64)	なし／SP1	9.0.0.0～	9.0.0.0～	4.7.4～
	Datacenter	なし／SP1	9.0.0.0～	9.0.0.0～	4.7.4～

推奨スペックは、LanScope Catが以下の構成の場合を前提として算出しています。
製品構成：プレミアムパック（アセット・ログ[アプリ通信ログ取得あり※]・ウェブ・デバイス・ID監査・メール） データ保存日数：システムデータ[95日]、ログ検索データ[5年]
※アプリ通信ログの保存領域として、100台の場合は90GB、500台の場合は500GBを見込んでいます。

利用中のLanScope CatマネージャーへL2Blockerマネージャーを追加インストールできます。インストール手順はL2Blockerの「マネージャーセットアップガイド」をご参照ください。LanScope CatとL2Blockerを同時にインストールする場合には、LanScope Catを先にインストールしてください。

L2Blocker価格表

●LanScope Cat 不正接続防止ツール L2BlockerマネージャーVer.4

※管理ネットワークごとに購入必須

製品名	製品型式	製品単価	保守年数	保守型番	保守単価
LanScope Cat不正接続防止ツール L2Blockerマネージャー Ver.4	Cat/L2V4-MGR	¥240,000	単年保守	Cat/L2V4-MGR-M	¥28,800
			4年保守	Cat/L2V4-MGR-4Y	¥76,800

※初年度保守費用は製品価格に含みます。購入時点から最大5年まで利用可能

●LanScope Cat 不正接続防止ツール L2Blockerセンサー

製品名	製品単価	製品単価	保守年数	保守型番	保守単価
スタンダード版	Cat/L2V4-SEN-ST	¥140,000	単年保守	Cat/L2V4-SEN-ST-M	¥16,800
			4年保守	Cat/L2V4-SEN-ST-4Y	¥44,800
タグVLAN版	Cat/L2V4-SEN-TUG	¥340,000	単年保守	Cat/L2V4-SEN-TUG-M	¥40,800
			4年保守	Cat/L2V4-SEN-TUG-4Y	¥108,800

※初年度保守費用は製品価格に含みます。購入時点から最大5年まで利用可能、5年経過後は買い直し
※スタンダード版：1セグメントごとに1つのセンサーが必要 タグVLAN版：1つのセンサーで32VLANを管理可能
※保守型番は、購入時から最大5年間まで利用可能。初年度保守費用は製品価格に含まれており、次年度以降の更新時に利用。もしくは故障時の代替機の提供

●LanScope Cat 不正接続防止ツール L2Blockerラックマウントキット

製品名	製品型式	製品単価
LanScope Cat不正接続防止ツール L2Blocker ラックマウントキット	Cat/L2V4-RACK	¥25,000

※L2Blockerセンサーの別途購入が必須（スタンダード版・タグVLAN版共通）

導入事例

L2Blocker導入事例／L2Blocker×LanScope Cat事例

クラウドで導入・管理が容易な端末管理 管理者不在拠点にも本社同等のセキュリティ

L2Blokерで拠点のセキュリティとガバナンスを実現



業種

サービス業

導入

L2Blokер（クラウド版）

効果

セキュリティ強化／一元管理

【運用における課題】

標的型攻撃増加で狙われる拠点のセキュリティ強化

サイバー攻撃が増えている中、本社よりも拠点の方がリスクが大きくなり本社と同等以上のセキュリティが必要と感じ検討。

加えて各拠点の規模は10台前後のため、兼任業務でも簡単に導入、運用できるものが条件。

【L2Blokерで課題解決】

クラウド版を選択する事で国内外を管理者不在でも一元管理

本社から送った設定済のセンサーをネットワークに繋ぐだけで監視スタート。L2Blokер管理下の国内外のネットワークの状況はクラウドを介し一つの管理画面上で一括管理が可能。

業務上お客様との間で発生する無線LAN経由の接続に関してはMACアドレス認証で精査をかけ、ガバナンスを強化。

ユーザーが求めている IT資産管理運用を実現

他拠点のネットワーク管理にLanScope Cat×L2Blocker



業種

製造業

導入

LanScope Cat／L2Blocker

効果

セキュリティ強化／一元管理

【運用における課題】

様々なITリテラシーの従業員のIT資産管理を徹底

不正検知機能を社員の端末に持たせてしまっていたため、該当社員の帰宅後は私物端末を自由に利用されていた。

管理ができているか不明瞭だったため、夜使えたのは昼は接続できないという問い合わせが増加し、**問い合わせ対応に追われる課題**が発生。

【L2Blockerで課題解決】

管理下に置くことで安定稼働が実現。問い合わせも激減

専用のハードウェアのため**24時間不正な接続を防止**することが可能となり、安定的に管理ができた。

無断接続機器に対して**Webブラウザを介して通知し把握**する体制が構築

今の環境を変えず置くだけ24時間365日 コスト抑えながらセキュリティを担保

Pushで行う不正LanScope Cat×L2Blocker



業種

製造業

導入

LanScope Cat／L2Blocker

効果

セキュリティ強化／コスト対策

【運用における課題】

複数拠点をできるだけコストを抑え対策

これまで現状把握はできていたものの実際に制御などは行っておらず、セキュリティ面に不安があったため、不正な接続を監視・制御できるソリューションを検討。

拠点多く、ネットワーク数が多いのがネックとなっており、通常の遮断ソリューションではコスト面が合わず、元々Catを導入していたためどうかできないか相談。

【Cat×L2Blockerで課題解決】

取り扱う情報や業務によって使い分け

管理を2段階に分けて構築。業務で機密情報を取り扱ったり、人の出入りが多い環境に対してL2Blockerを導入し、監視体制を整えた。それ以外は遮断キャットを導入し、必要最低限のシンプルな管理にすることで、コストを抑えつつ必要な遮断体制が実現。

なにより、アプライアンスのため電源など気にせず24時間365日監視してくれるのが安心感につながっている。

全国複数拠点をハイブリッド一元管理 大規模ネットワークの効率管理でITインフラ整備

L2Bloker×Catで常に正常なITインフラを維持



業種

建設・運輸業

導入

LanScope Cat／L2Bloker

効果

セキュリティ強化／一元管理

【運用における課題】

複数にわたる大規模ネットワークの一元管理

不正接続対策システムの更改に伴い、ネットワークに接続が許可されていない機器のネットワーク通信の防止、及び接続行為の検知を実現することを目的に様々な製品を調査。

全国に約70拠点、全部で約130セグメントの一元管理を検討。

【Cat×L2Blokerで課題解決】

管理下に置くことで安定稼働が実現。問い合わせも激減

L2Bを採用することで、**複数セグメント（VLANを含む）も一元管理**ができるようになり、効率的な管理が行えるようになった。

導入済のCatと連携させることで、**Cat未導入の管理外PCを察知・対応**することで、ITインフラ全体の管理が実現できた。

【参考】今すぐできる不正遮断L2Bloker導入には支援制度を活用してください

国・行政からの支援制度も多数！この機会におトクにセキュリティ対策しませんか

IT導入補助金

主幹組織：経済産業省

制度概要

中小企業を対象に、生産性向上に寄与するIT投資に対して補助。新型コロナウイルスの感染拡大対策として、テレワーク整備などに取り組む事業者を優先的に支援するため、特別枠（C類型）を創設。

補助金額

補助額の上限：30万～450万円

補助率：3/4

<https://www.it-hojo.jp/>

サイバーセキュリティ対策促進助成金

主幹組織：東京都中小企業振興公社

制度概要

中小企業等が自社の企業秘密や個人情報等を保護する観点から構築したサイバーセキュリティ対策を実施するための設備等の導入を支援。

補助金額

補助率：1/2

補助額：30万～1,500万円

<https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html>

MOTEX限定キャンペーン

不正接続をキャッチ！

ハイブリッド勤務のシンプルセキュリティに最適！ L2Bloker **38%OFF** キャンペーン

忙しい管理者の代わりに「場所」「時間」を問わないセキュリティの初期対応！

キャンペーン実施期間：2020年9月30日発注分まで

24時間365日監視するアプライアンスを特別価格でご提供！

初めてL2Blokerを導入する方対象です！アプライアンスなので現在の環境は変更せず使えます。

Cat導入済の場合、管理下にあるPCは自動で接続許可されるので、管理も簡単です。



●製品本体（サーバーIN）

L2Bloker

通常価格：240,000円が

148,800円

●スタンダード版



通常価格：140,000円が

86,800円

●タグVLAN



通常価格：340,000円が

210,800円

【キャンペーン詳細・お申し込みはこちら】

<https://www.lanscope.jp/cat/campaign/l2blocker/>

20分で分かる！

L2Blocker

×

LanScope **Cat**

で実現！

テレワーク×オフィスワークStyle企業が やっておくべきセキュリティ対策ポイント4選

多忙な情シスさん必見！究極のシンプルセキュリティ



問合せ多数！L2Blockerの定期Webiner開催中です

緊急事態宣言も解除されゆっくりと日常が戻りつつある今、我々の働き方は新しい時代を迎えようとする中、オフィスワークStyleにとらわれないハイブリッド勤務を検討する企業が増えています。そこで気を付けておきたのがセキュリティ対策です。テレワーク対策として緊急で導入した機器やルールが、対策不足により徐々にセキュリティホール化しています。本セミナーでは、新しい働き方におけるセキュリティ課題をご紹介しますと共に、シンプルに解決するための「L2Blocker」活用方法をご紹介します。忙しい情シスさんにぴったり！究極のシンプルセキュリティです。

●詳細・お申し込みはこちら

<https://go.motex.co.jp/l/320351/2020-06-23/3f9cqb>





お問い合わせ先

東京本部 : 03-5460-1371

大阪本社 : 06-6308-8980

名古屋支店 : 052-253-7346

九州営業所 : 092-419-2390

E-Mail : sales@motex.co.jp

<http://www.motex.co.jp>