LANSCOPE

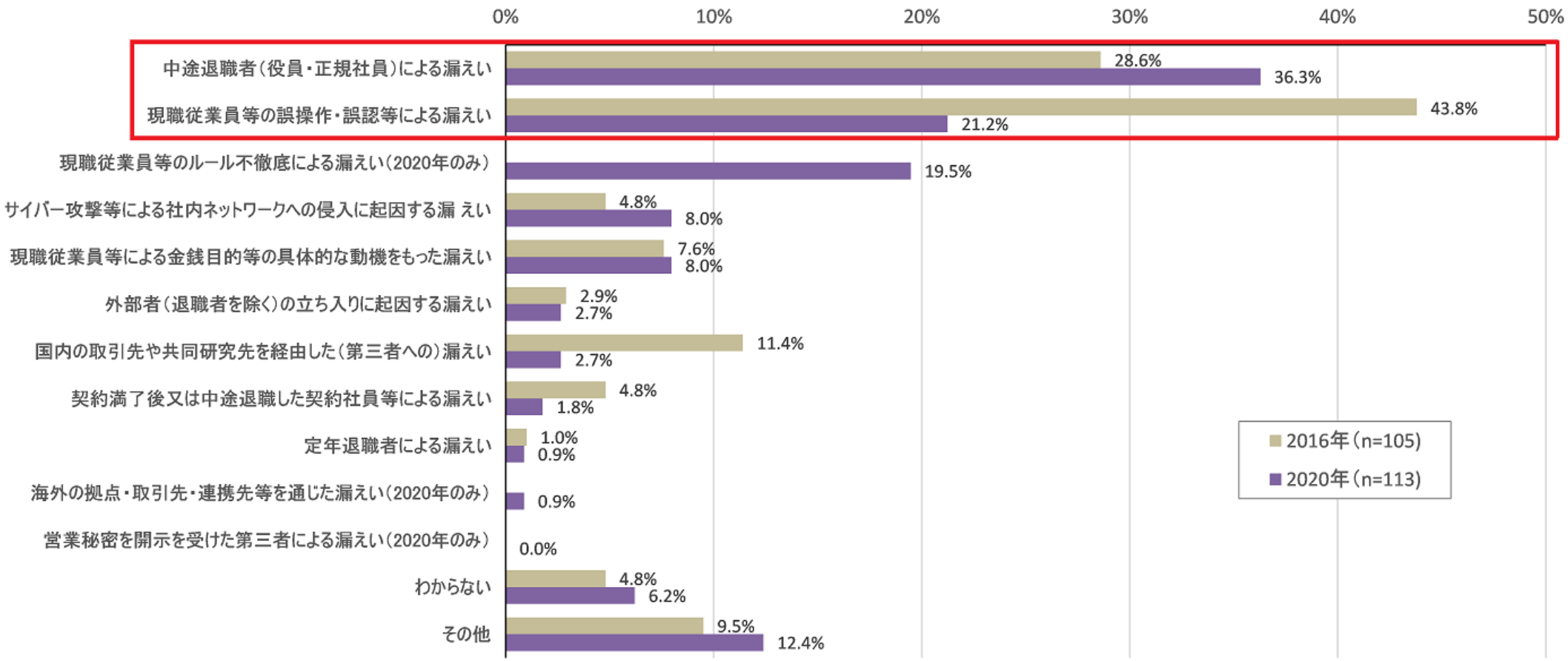
知らなかったでは済まされない！

改正個人情報保護法に備える

急増する内部不正による情報漏えい

価値がある情報が故に社内や関係者からの悪意のある情報漏えいが急増しています

外部指摘で初めて発覚するケースも・・・自社のみならず委託先やグループ内など範囲が広いケースが増加



※引用IPA「企業における営業秘密管理に関する実態調査2020」報告書

改正の目的

社会情勢に合わせて３年ごとに見直し！2020年6月に改正個人情報保護法が公布されました

2005年4月に「個人情報」を保護するための法律として「個人情報保護法」が施行。その後も平成27年の個人情報保護法の改正以来、社会情勢の変化に伴い見直しが行われています。今回の改正は、令和元年１月に示した「３年ごと見直しに係る検討の着眼点」に即し、３年ごとに個人情報保護法の見直しを受け、反映したものです。

見直しの基準となる５つの視点

個人の
権利利益保護

外国事業者による
リスク変化への対応

保護と利用の
バランス

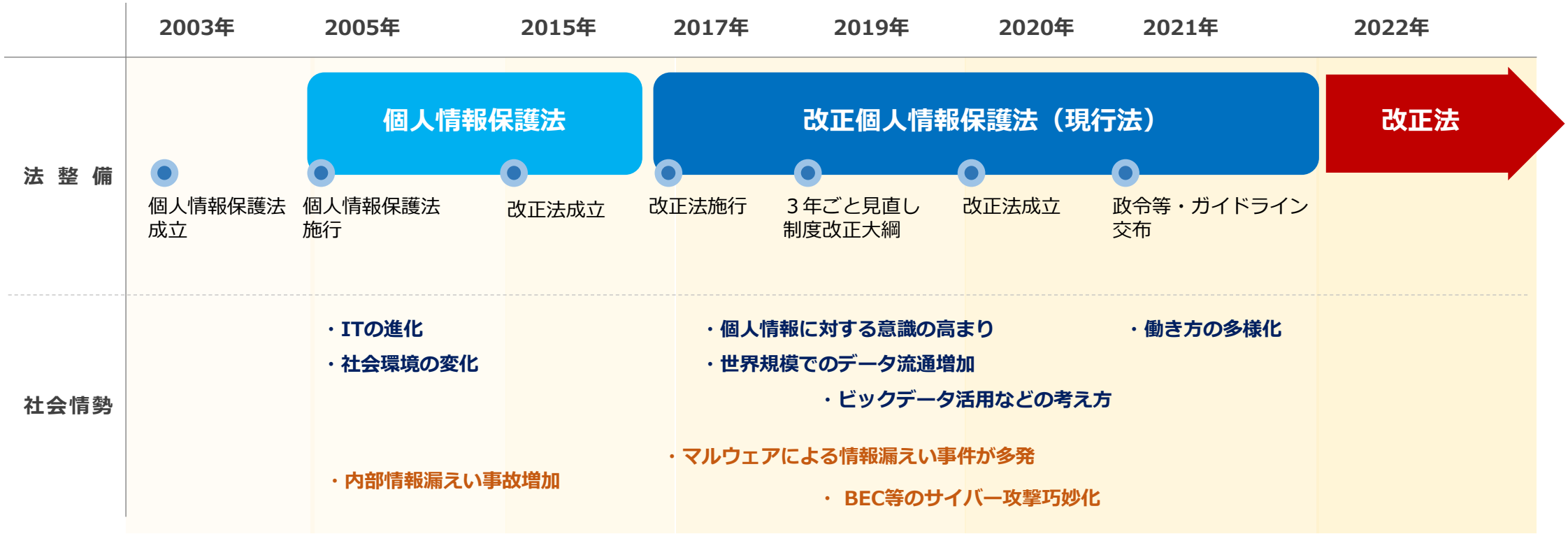
AI・ビッグデータ時代
への対応

国際的潮流との
調和

※引用元：PPC個人情報保護委員会「個人情報保護法 いわゆる３年ごと見直し 制度改正大綱（概要）

改正の流れ

「個人情報保護法」は社会情勢を受けて進化！罰則化されるなど経営側も対応していく必要があります



対策すべきは、改正個人情報保護法（個人情報の保護に関する法律等の一部を改正する法律）

交布日：2020年6月12日　　施行日：2022年4月1日

そもそも個人情報とは

「個人情報」の定義は、改正個人情報保護法で定義がより詳細になりました

第二条 この法律において「個人情報」とは、生存する個人に関する情報であって、 次の各号のいずれかに該当するものをいう。

一 当該情報に含まれる氏名、生年月日その他の記述等**（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。 次項第二号において同じ。）で作られる記録をいう。第十八条第二項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）**により特定の個人を識別することができるもの （他の情報と容易に照合することができ、それにより特定の個人を識別することが できることとなるものを含む。）

二 個人識別符号が含まれるもの

※引用：個人情報保護委員会事務局「改正個人情報保護法の基本」

個人識別符号とは

身体の一部の特徴を電子計算機のために変換した符号

（ＤＮＡ、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋、掌紋）

サービス利用や書類において対象者ごとに割り振られる公的な番号

（旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー等）

改正個人情報保護法の６つのポイント！漏えい時の報告義務の強制とペナルティ制度が強化されています

1	個人の権利の在り方	利用停止・消去等の個人の請求権について、個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和する。保有個人データの開示方法について、電磁的記録の提供を含め、本人が指示できるようにする。個人データの授受に関する第三者提供記録について、本人が開示請求できるようにする。６ヶ月以内に消去する短期保存データについて、保有個人データに含めることとし、開示、利用停止等の対象とする。オプトアウト規定により第三者に提供できる個人データの範囲を限定し、①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外とする。
2	事業者の義務の在り方	漏えい等が発生し、個人の権利利益を害するおそれがある場合に、委員会への報告及び本人への通知を義務化する。違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨を明確化する。
3	自主的な取組の仕組み	認定団体制度について、現行制度に加え、企業の特定分野(部門)を対象とする団体を認定できるようにする。
4	データ利活用の施策	イノベーションを促進する観点から、氏名等を削除した「仮名加工情報」を創設し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和する。提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務付ける。
5	ペナルティの強化	委員会による命令違反・委員会に対する虚偽報告等の法定刑を引き上げる。データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、法人に対しては行為者よりも罰金刑の最高額を引き上げる（法人重科）
6	法の域外適用・越境移転	日本国内にある者に係る個人情報等を取り扱う外国事業者を、罰則によって担保された報告徴収・命令の対象とする。外国にある第三者への個人データの提供時に、移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等を求める。

※引用：個人情報保護委員会事務局「改正個人情報保護法の基本」https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf

2.事業者の義務が追加

情報漏えい時の報告が努力義務から義務化！現在のプライバシーポリシーの見直しが急務です

漏えい等が発生した時
個人情報保護法委員会と本人への通知が義務化

質的に侵害のおそれが大きい類型と、量的に侵害のおそれが大きい類型が報告等義務の対象となります。報告の方法も速報と確報に分けて報告することが求められています。

違法や不当な行為を助長する不適正な方法により
個人情報を利用してはならない旨が義務化

利用目的の範囲内での利用という制限に加え、違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならないことが義務化されました。

公表等事項として、事業者の住所及び代表者の氏名・
安全管理措置の内容・利用目的の特定の充実が追加

事業者の住所や法人の場合における代表者の氏名が公表等事項に追加、事業者が保有個人データについて講じている安全管理措置の内容も、改正法の施行令において公表等事項に加えられました。

報告が求められる例

「質的」「量的」に侵害の恐れが大きい類型に対して報告が求められています

単に漏えいしたデータ数だけで判断するのではなく、個人の権利利益に対する影響が大きいと考えられる、個人データの性質・内容、規模等が考慮されています

事態の類型	漏えい等報告・本人通知が必要となる場合	件数	例外
個人データの性質	要配慮個人情報の漏えい（おそれも含む）	１件以上	「高度な暗号化等の秘匿化」がされた個人データ
個人データの内容	財産的被害が発生するおそれがある場合（例：クレジットカード番号やインターネットバンキングのＩＤ・パスワード等）（おそれも含む）	―	
漏えい等の態様	故意による漏えい（例：不正アクセスや従業員による持ち出し等）（おそれも含む）	―	
大規模な漏えい	個人データの性質・内容、漏えい等の態様を問わず、大規模な個人データの漏えい	1000件以上	
漏えい等のおそれ	上記のおそれがある場合	―	

要配慮個人情報

本人の人種、信条、社会的身分、病歴、犯罪 の経歴、犯罪により害を被った事実など

財産的被害が発生するおそれがある場合

クレジットカード番号やインターネットバンキングのID・パスワード情報など

故意による漏えい

類型的に二次被害が発生するおそれがある不正アクセスや従業員による持ち出しなど

大規模な情報漏えい

内容が個人情報でなくても一定数以上の大規模な漏えい※1000人を基準

「おそれ」がある場合

漏えいの懸念があり漏えいが確定していない段階
※被害を最小限に

法定刑が個人・法人共に概ね引き上げ！特に法人の罰金刑の上限額が大きく引き上げられました

措置命令・報告義務違反の罰則について法定刑を引き上げ　/　法人に対する罰金刑を引き上げ

命令違反や虚偽の報告を抑止する効果を見越し、法定刑の引き上げが実施、特に法人は罰金刑が大幅に引き上げられています。

■ 改正前後の法定刑の比較

表1 改正前後の法定刑の比較

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会 からの命令への違反	行為者	６月以下	**１年以下**	３０万円以下	**100万円以下**
	法人等	-	-	３０万円以下	**１億円以下**
個人情報データベース等の不正提供等	行為者	１年以下	１年以下	５０万円以下	５０万円以下
	法人等	-	-	５０万円以下	**１億円以下**
個人情報保護委員会 への虚偽報告等	行為者	-	-	３０万円以下	**５０万円以下**
	法人等	-	-	３０万円以下	**５０万円以下**

※引用：個人情報保護委員会「令和２年 改正個人情報保護法について」https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/

個人情報保護のために必要な４つの「安全管理措置」が掲げられています

事業者が個人情報の漏えいや滅失などの防止等のためにもうけられたのが「安全管理措置」（個人情報保護法20条）です

8-3 **組織的安全管理措置**	（1）組織体制の整備　（2）個人データの取扱いに係る規律に従った運用 （3）個人データの取扱状況を確認する手段の整備　（4）漏えい等の事案に対応する体制の整備 （5）取扱状況の把握及び安全管理措置の見直し
8-4 **人的安全管理措置**	従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。
8-5 **物理的安全管理措置**	（1）個人データを取り扱う区域の管理　（2）機器及び電子媒体等の盗難等の防止 （3）電子媒体等を持ち運ぶ場合の漏えい等の防止　（4）個人データの削除及び機器、電子媒体等の廃棄
8-6 **技術的安全管理措置**	（1）アクセス制御　（2）アクセス者の識別と認証　（3）外部からの不正アクセス等の防止 （4）情報システムの使用に伴う漏えい等の防止

情報を安全に保全するために、組織的にルールや体制構築することが求められています

（1） 組織体制の整備	**安全管理措置を講ずるための組織体制を整備しなければならない。** ・個人データの取扱いに関する責任者の設置及び責任の明確化　・個人データを取り扱う従業者及びその役割の明確化 ・上記の従業者が取り扱う個人データの範囲の明確化　・個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化 ・個人データの漏えい等の事案の発生又は兆候を把握した場合の責任者への報告連絡体制 ・法や個人情報取扱事業者で整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合の責任者への報告連絡体制
（2） 個人データの取扱いに係る規律に従った運用	**あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。** ・整備された個人データの取扱いに係る規律に従った運用の状況を確認するため、利用状況等を記録することも重要である。 ・個人情報データベース等の利用・出力状況　・個人データが記載又は記録された書類・媒体等の持ち運び等の状況 ・個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。） ・個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）
（3） 個人データの取扱状況を確認する手段の整備	**個人データの取扱状況を確認するための手段を整備しなければならない。** ・個人情報データベース等の種類、名称　・個人データの項目　・責任者・取扱部署　・利用目的　・アクセス権を有する者 等
（4） 漏えい等の事案に対応する体制の整備	**漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。** ・漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である・事実関係の調査及び原因の究明 ・影響を受ける可能性のある本人への連絡　・個人情報保護委員会等への報告　・再発防止策の検討及び決定　・事実関係及び再発防止策等の公表等
（5） 取扱状況の把握及び安全管理措置の見直し	**個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。** ・個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。・外部の主体による監査活動と合わせて、監査を実施

従業者に個人データの適正な取扱いを周知徹底・教育することを求められています

従業者の教育	・個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行う。 ・個人データについての秘密保持に関する事項を就業規則等に盛り込む。

個人情報の取り扱いに関わる機器をセキュアに管理するためのルール・体制構築が求められています

（1） 個人データを取り扱う区域の管理	**個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域及びその他の個人データを取り扱う事務を実施する区域について、それぞれ適切な管理を行わなければならない。** ・入退室管理及び持ち込む機器等の制限等。入退室管理の方法としては、IC カード、ナンバーキー等による入退室管理システムの設置等が考えられる。 　└間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止
（2） 機器及び電子媒体等の盗難等の防止	**個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行わなければならない。** ・個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。 ・個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。）
（3） 電子媒体等を持ち運ぶ場合の漏えい等の防止	**個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない。** ・持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。 ・封緘、目隠しシールの貼付けを行う。・施錠できる搬送容器を利用する。
（4） 個人データの削除及び機器、電子媒体等の廃棄	**個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行わなければならない。また、個人データを削除した場合、又は、個人データが記録された機器、電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存することや、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認することも重要である。** ・（個人データが記載された書類等を廃棄する方法の例）焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。 ・（個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄する方法の例）情報システム（パソコン等の機器を含む。）において、個人データを削除する場合、容易に復元できない手段を採用する。 ・個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する。

個人データ自体に対してセキュアに管理を行うためのルール・体制構築が求められています

（1） アクセス制御	**担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない。** ・個人情報データベース等を取り扱うことのできる情報システムを限定する。 ・情報システムによってアクセスすることのできる個人情報データベース等を限定する。 ・ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。
（2） アクセス者の 識別と認証	**個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。** ・（情報システムを使用する従業者の識別・認証手法の例）ユーザーID、パスワード、磁気・ICカード等
（3） 外部からの 不正アクセス等の防止	**個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。** ・情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 ・情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入し、不正ソフトウェアの有無を確認する。 ・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ・ログ等の定期的な分析により、不正アクセス等を検知する。
（4） 情報システムの使用に 伴う漏えい等の防止	**情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。** ・情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。）。 ・個人データを含む通信の経路又は内容を暗号化する。 ・移送する個人データについて、パスワード等による保護を行う。

2022年施行のポイント

個人情報の取り扱いが厳格化、漏えい時には通知が「完全義務化」され「厳罰」が科されます

従来の「個人情報保護法」で定められたガイドラインに加え、時勢を踏まえレビジョンアップされました

1. 情報漏えい時の通知が、**努力義務** から **完全義務化** へ

2. 報告は **速報** と **確報** の二段階で報告

3. 罰則引き上げ！ 法人は **最大１億円** の罰則

LANSCOPEで対応できる改正個人情報保護法対策

情報漏えいをさせない体制と、万が一の対策

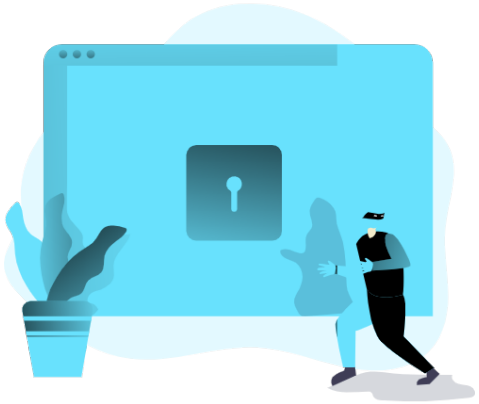
LANSCOPEは情報漏えいをさせない「体制構築」と「万が一の対応」が可能です

「安全管理措置」で求められている講ずべき措置に対し、様々な対策が行えます

内部情報漏えい対策

「組織的安全管理措置」「技術的安全管理措置」対応として誰が・どのデータに対し・何を行ったか**操作履歴を取得、問題操作をリアルタイムに察知・対策する**ことで情報漏えいをさせないための体制づくりを支援します。

外部脅威対策



「技術的安全管理措置」対応として、常に最新のバージョンを保てているかどうか、**脆弱性の有無を可視化**。対策することでセキュリティホールを無くし、外部からの脅威対策を打つことが可能です。

セキュリティ啓蒙

「人的安全管理措置」対応として、従業員に対する**セキュリティ教育で周知・教育・訓練**するための様々な啓蒙コンテンツを提供しています。

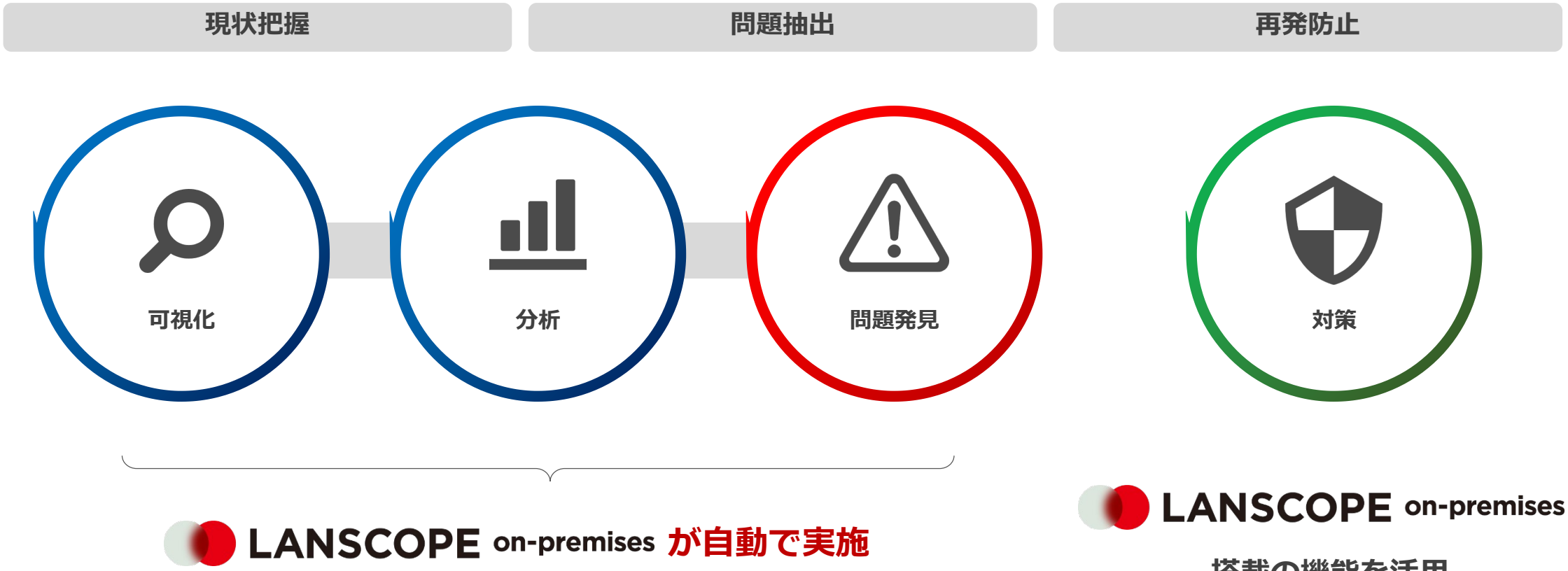
内部情報漏えい対策

IT資産管理・操作ログ管理

内部情報漏えい対策

対策すべき問題点を自動で抽出！対策はLANSCOPEの多彩な機能で実施します

大量のログから検索して探す必要はありません。対策すべき問題操作のみを抽出・お知らせしますので管理工数も大幅に軽減されます



内部情報漏えい対策

ネットワーク上の接続機器を検出！不明な機器の接続をリアルタイムで検知・遮断することが可能

検知は３つのゾーンで管理が可能で、管理下にない不正な接続を察知・遮断することが可能です

A 導入環境

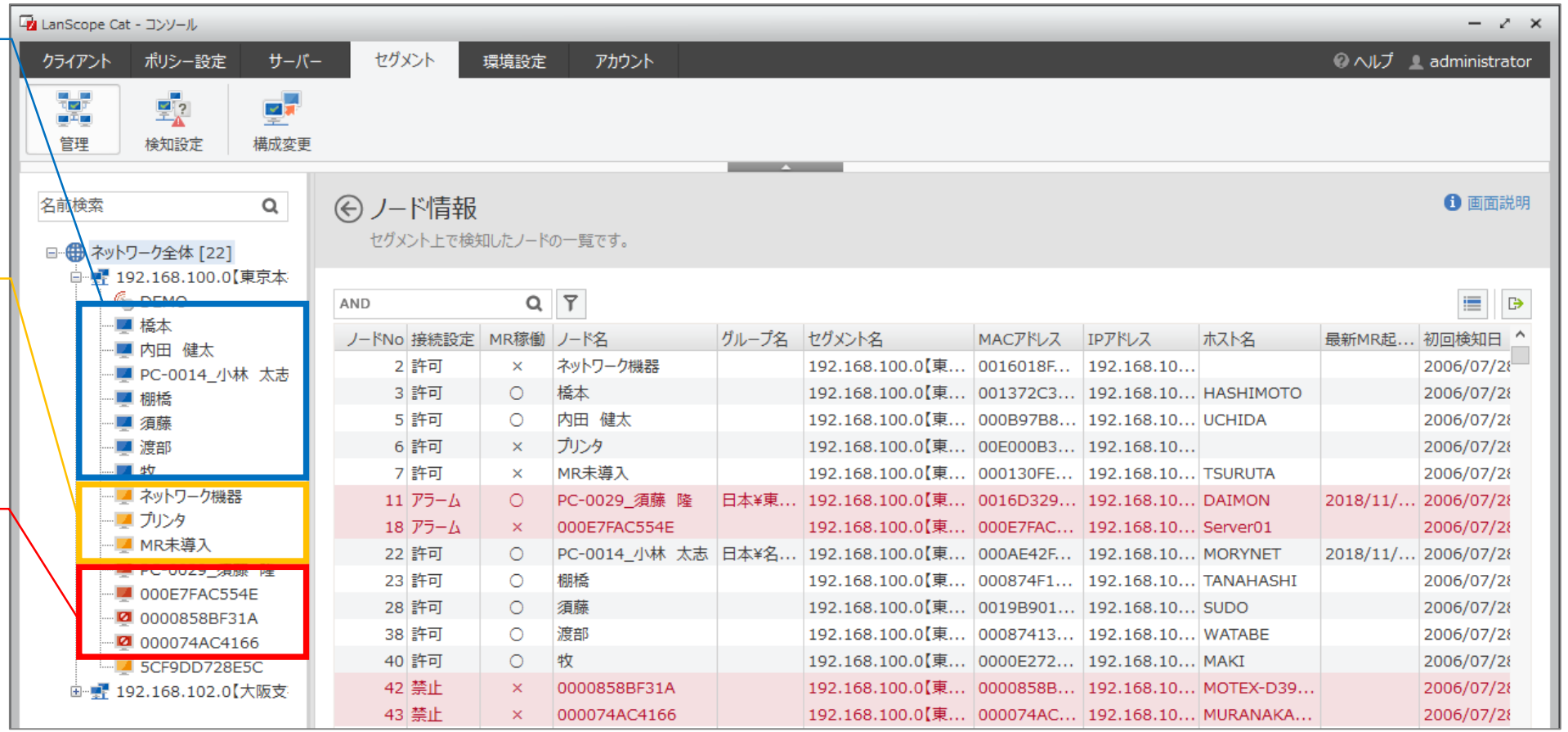
LANSCOPEを
導入している環境

B 社内PC

会社に必要な
ネットワーク機器

C 不正PC検知

管理者が把握してない
未導入の環境



ノードNo	接続設定	MR稼働	ノード名	グループ名	セグメント名	MACアドレス	IPアドレス	ホスト名	最新MR起...	初回検知日
2	許可	×	ネットワーク機器		192.168.100.0【東...	0016018F...	192.168.10...			2006/07/28
3	許可	○	橋本		192.168.100.0【東...	001372C3...	192.168.10...	HASHIMOTO		2006/07/28
5	許可	○	内田　健太		192.168.100.0【東...	000B97B8...	192.168.10...	UCHIDA		2006/07/28
6	許可	×	プリンタ		192.168.100.0【東...	00E000B3...	192.168.10...			2006/07/28
7	許可	×	MR未導入		192.168.100.0【東...	000130FE...	192.168.10...	TSURUTA		2006/07/28
11	アラーム	○	PC-0029_須藤　隆	日本¥東...	192.168.100.0【東...	0016D329...	192.168.10...	DAIMON	2018/11/...	2006/07/28
18	アラーム	×	000E7FAC554E		192.168.100.0【東...	000E7FAC...	192.168.10...	Server01		2006/07/28
22	許可	○	PC-0014_小林　太志	日本¥名...	192.168.100.0【東...	000AE42F...	192.168.10...	MORYNET	2018/11/...	2006/07/28
23	許可	○	棚橋		192.168.100.0【東...	000874F1...	192.168.10...	TANAHASHI		2006/07/28
28	許可	○	須藤		192.168.100.0【東...	0019B901...	192.168.10...	SUDO		2006/07/28
38	許可	○	渡部		192.168.100.0【東...	00087413...	192.168.10...	WATABE		2006/07/28
40	許可	○	牧		192.168.100.0【東...	0000E272...	192.168.10...	MAKI		2006/07/28
42	禁止	×	0000858BF31A		192.168.100.0【東...	0000858B...	192.168.10...	MOTEX-D39...		2006/07/28
43	禁止	×	000074AC4166		192.168.100.0【東...	000074AC...	192.168.10...	MURANAKA...		2006/07/28

LANSCOPE連携製品
L2Blocker

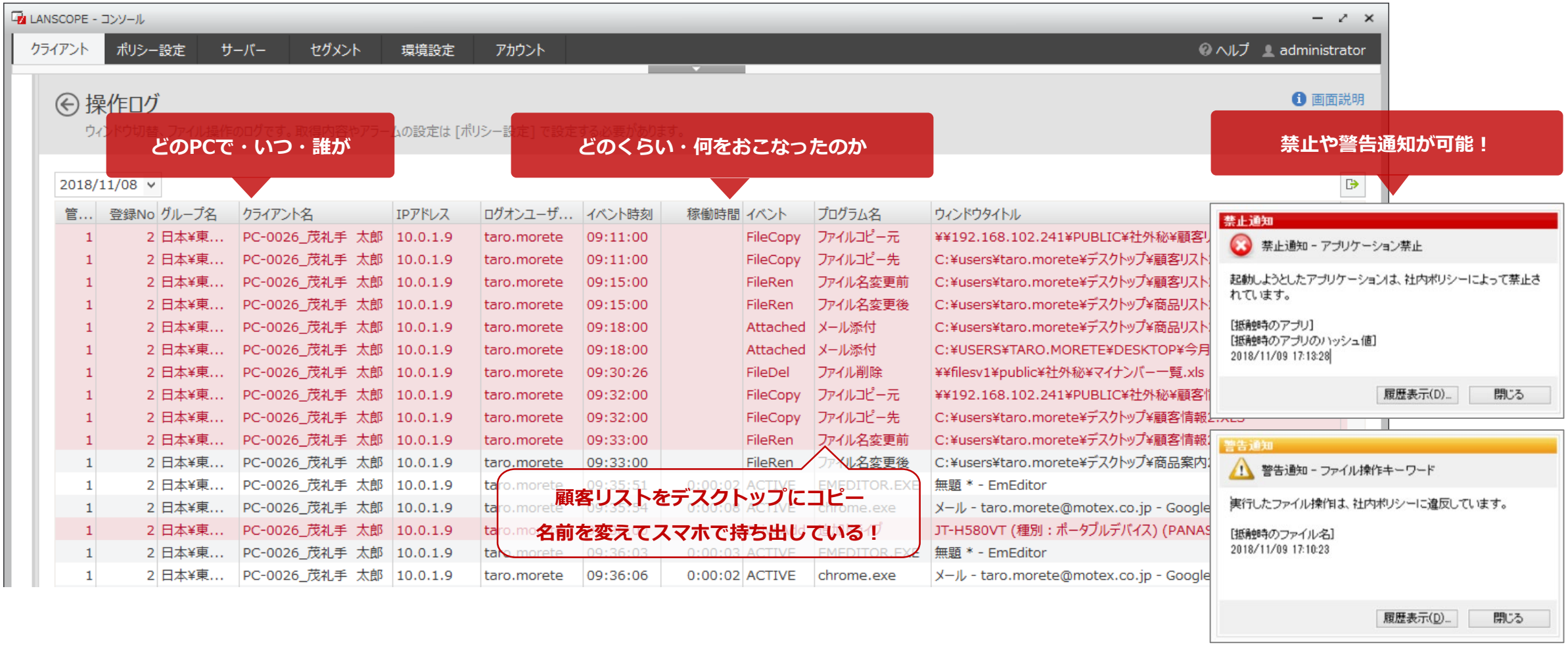
ネットワーク遮断に特化したアプライアンス型の検知・遮断製品です。最大で３２セグメントが検知可能なためコスト高になりがちな遮断ソリューションのコストを大幅に抑えることも可能です。

内部情報漏えい対策

正しい操作を証明するための証跡や、違反操作があった場合、ユーザーや管理者に通知し抑止効果

どのPCで・誰が・いつ・どんな操作をしたかを記録し、万が一情報漏えいが発生した際に報告に活用できます

●操作ログ画面



管...	登録No	グループ名	クライアント名	IPアドレス	ログオンユーザ...	イベント時刻	稼働時間	イベント	プログラム名	ウィンドウタイトル
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:11:00		FileCopy	ファイルコピー元	¥¥192.168.102.241¥PUBLIC¥社外秘¥顧客リ
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:11:00		FileCopy	ファイルコピー先	C:¥users¥taro.morete¥デスクトップ¥顧客リスト
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:15:00		FileRen	ファイル名変更前	C:¥users¥taro.morete¥デスクトップ¥顧客リスト
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:15:00		FileRen	ファイル名変更後	C:¥users¥taro.morete¥デスクトップ¥商品リスト
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:18:00		Attached	メール添付	C:¥users¥taro.morete¥デスクトップ¥商品リスト
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:18:00		Attached	メール添付	C:¥USERS¥TARO.MORETE¥DESKTOP¥今月
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:30:26		FileDel	ファイル削除	¥¥filesv1¥public¥社外秘¥マイナンバー一覧.xls
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:32:00		FileCopy	ファイルコピー元	¥¥192.168.102.241¥PUBLIC¥社外秘¥顧客情
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:32:00		FileCopy	ファイルコピー先	C:¥users¥taro.morete¥デスクトップ¥顧客情報
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:33:00		FileRen	ファイル名変更前	C:¥users¥taro.morete¥デスクトップ¥顧客情報
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:33:00		FileRen	ファイル名変更後	C:¥users¥taro.morete¥デスクトップ¥商品案内
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:35:51	0:00:02	ACTIVE	EMEDITOR.EXE	無題 * - EmEditor
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:35:54	0:00:03	ACTIVE	chrome.exe	メール - taro.morete@motex.co.jp - Google
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete					JT-H580VT (種別：ポータブルデバイス) (PANAS
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:36:03	0:00:03	ACTIVE	EMEDITOR.EXE	無題 * - EmEditor
1	2	日本¥東...	PC-0026_茂礼手 太郎	10.0.1.9	taro.morete	09:36:06	0:00:02	ACTIVE	chrome.exe	メール - taro.morete@motex.co.jp - Google

内部情報漏えい対策

対策すべき問題操作（アラーム）のみを自動抽出！ルール違反の有無をひと目で確認

問題操作を日付ごとに組織単位や人単位で集計し、大量のログの中から確認すべき「問題自体」が発生しているのかどうかを視覚的に把握

内部情報漏えい対策

問題操作をお知らせするアラーム設定は対策したい項目にチェックを付けるだけのカンタン設定

ルールを一から考えなくてOK！セキュリティリスクの可能性がある操作に対し、リアルタイムに検知・通知することが可能です

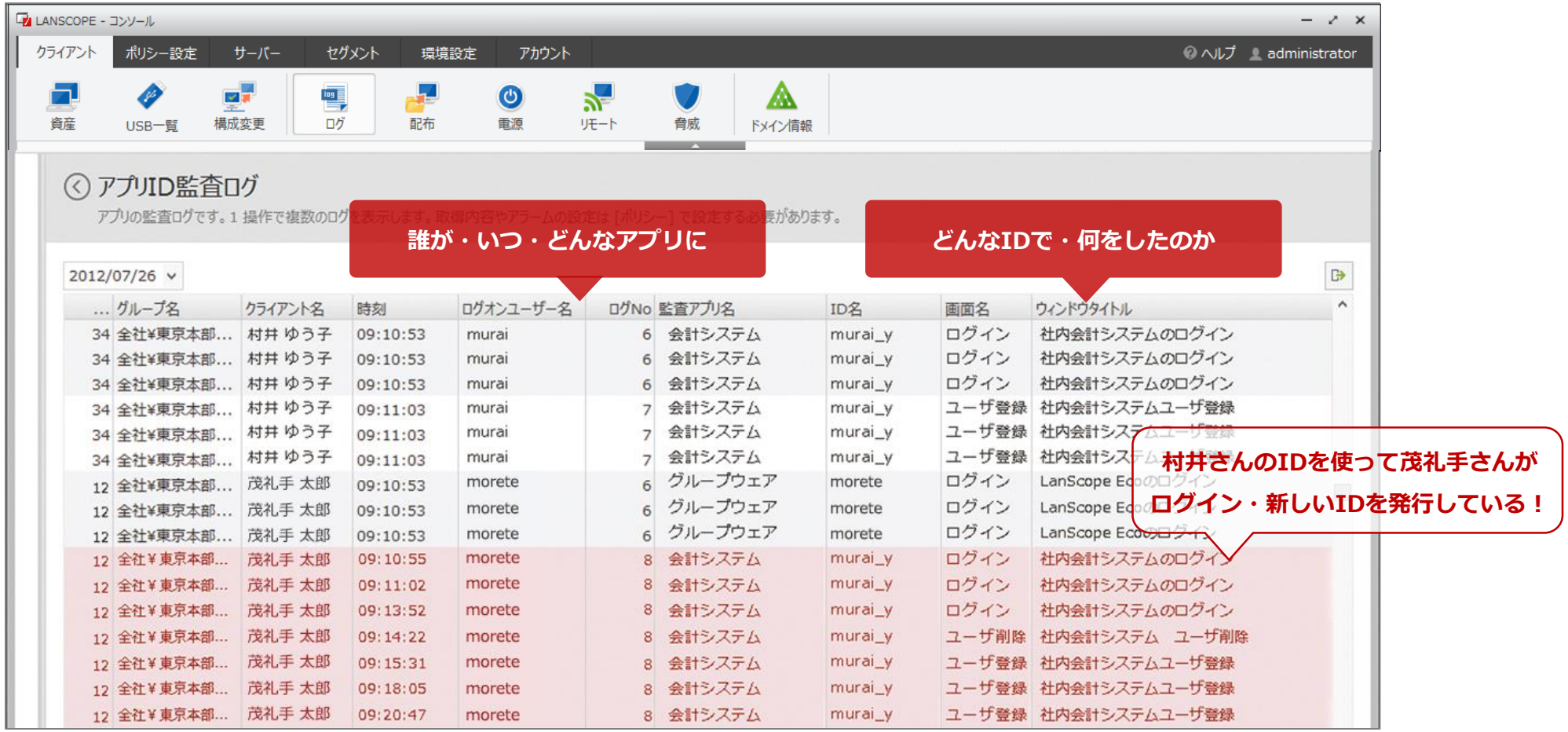
	アラーム	ポリシー	項目	禁止
資産	資産	資産ポリシー	IP アドレスの重複／変更	–
			コンピューター名変更	–
			NIC ／ SCSI ／モデムの変更	–
			DMI ハードウェア情報の変更	–
			CPU ／メモリサイズの変更	–
			MAC アドレスの変更	–
			日時の変更	–
			リース切れ	–
			新規アプリのインストール	–
			HDD 容量不足	–
	アプリ起動	アプリ稼働ポリシー	新規アプリの起動	–
	アプリ禁止	アプリ禁止ポリシー	禁止アプリの起動／名前変更	○
			レジストリエディタによる変更（禁止設定時）	○
			アプリのインストール（禁止設定時）	○
			システム構成の変更（禁止設定時）	○
	通信デバイス	通信デバイスポリシー	不許可通信デバイスの接続	○
効率	時間外	操作ポリシー	業務時間外の操作	–
		サーバー監視ポリシー		–
		アプリID 監査ポリシー		–

	アラーム	ポリシー	項目	禁止
行動	操作	操作ポリシー	機密フォルダーの操作	–
			CSVの出力	–
			USBメモリなどの外部メディアへの書き込み	–
			リモート PC への書き込み	–
			ローカル共有フォルダーの作成または書き込み	–
			ドライブの追加	–
			ウィンドウタイトルアラームに抵触	–
			メールの添付	–
			指定した条件に抵触するファイルの操作	–
	プリント	プリントポリシー	印刷枚数の超過	–
			キーワードに抵触したドキュメントの印刷	–
	Web	Web アクセスポリシー	指定したキーワード／ URL に抵触	○
			アップロード／ダウンロード	○
			Web への書き込み／ Webメールの送信	○
	ファイル操作	サーバー監視ポリシー	サーバーファイルの削除／アクセスの失敗	–
	接続失敗		サーバー接続の失敗	–
	不正接続	不正 PC 検知ポリシー	ネットワークへの不正な接続	–
	不正接続失敗		ネットワークへの不正な接続を禁止	○
	アプリ ID監査	アプリ ID 監査ポリシー	アプリの ID の作成／削除	–
			不許可設定した PC での操作	–
			操作回数アラームに抵触	–
	メール送信	メールポリシー	キーワードに抵触したメールの送信	–
脅威	脅威	–	マルウェアの検知	–
カスタム	カスタム	カスタムアラーム	カスタムアラームで指定した条件に抵触する操作	○

内部情報漏えい対策

システムのID利用を把握・監視！IDの使いまわしや悪用によるコンプライアンス違反を防止

基幹システム等のログインIDの利用を把握、IDの利用対策ができます。



…	グループ名	クライアント名	時刻	ログオンユーザー名	ログNo	監査アプリ名	ID名	画面名	ウィンドウタイトル
34	全社¥東京本部…	村井 ゆう子	09:10:53	murai	6	会計システム	murai_y	ログイン	社内会計システムのログイン
34	全社¥東京本部…	村井 ゆう子	09:10:53	murai	6	会計システム	murai_y	ログイン	社内会計システムのログイン
34	全社¥東京本部…	村井 ゆう子	09:10:53	murai	6	会計システム	murai_y	ログイン	社内会計システムのログイン
34	全社¥東京本部…	村井 ゆう子	09:11:03	murai	7	会計システム	murai_y	ユーザ登録	社内会計システムユーザ登録
34	全社¥東京本部…	村井 ゆう子	09:11:03	murai	7	会計システム	murai_y	ユーザ登録	社内会計システムユーザ登録
34	全社¥東京本部…	村井 ゆう子	09:11:03	murai	7	会計システム	murai_y	ユーザ登録	社内会計システム…
12	全社¥東京本部…	茂礼手 太郎	09:10:53	morete	6	グループウェア	morete	ログイン	LanScope Ecoのログイン
12	全社¥東京本部…	茂礼手 太郎	09:10:53	morete	6	グループウェア	morete	ログイン	LanScope Eco…
12	全社¥東京本部…	茂礼手 太郎	09:10:53	morete	6	グループウェア	morete	ログイン	LanScope Ecoのログイン
12	全社¥東京本部…	茂礼手 太郎	09:10:55	morete	8	会計システム	murai_y	ログイン	社内会計システムのログイン
12	全社¥東京本部…	茂礼手 太郎	09:11:02	morete	8	会計システム	murai_y	ログイン	社内会計システムのログイン
12	全社¥東京本部…	茂礼手 太郎	09:13:52	morete	8	会計システム	murai_y	ログイン	社内会計システムのログイン
12	全社¥東京本部…	茂礼手 太郎	09:14:22	morete	8	会計システム	murai_y	ユーザ削除	社内会計システム　ユーザ削除
12	全社¥東京本部…	茂礼手 太郎	09:15:31	morete	8	会計システム	murai_y	ユーザ登録	社内会計システムユーザ登録
12	全社¥東京本部…	茂礼手 太郎	09:18:05	morete	8	会計システム	murai_y	ユーザ登録	社内会計システムユーザ登録
12	全社¥東京本部…	茂礼手 太郎	09:20:47	morete	8	会計システム	murai_y	ユーザ登録	社内会計システムユーザ登録

「個人識別符号」と「個人情報」を的確に監視

LANSCOPE 連携製品を使えば、ファイルの内容や属性情報をもとに保管ルールに違反している個人情報ファイルを検出し対処を施す管理も可能です。

三菱スペース・ソフトウエア株式会社

すみずみ君

https://www.lanscope.jp/cat/product/partner/sumizumikun.html

アララ株式会社

P-Pointer FILE SECURITY

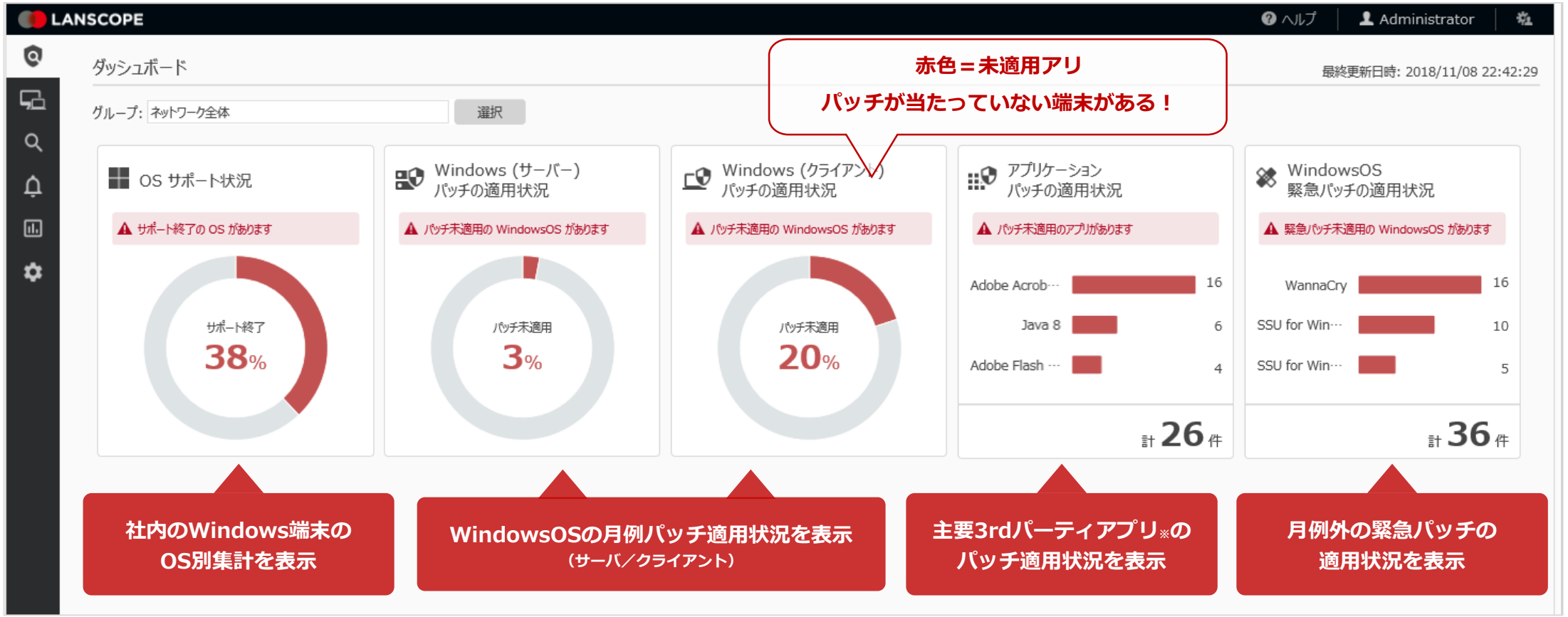
https://www.arara.com/news/press/entry4971/

外部脅威対策

脆弱性対策・マルウェア対策

脆弱性の有無をレポート！対策すべき脆弱性の可視化～対策までを支援

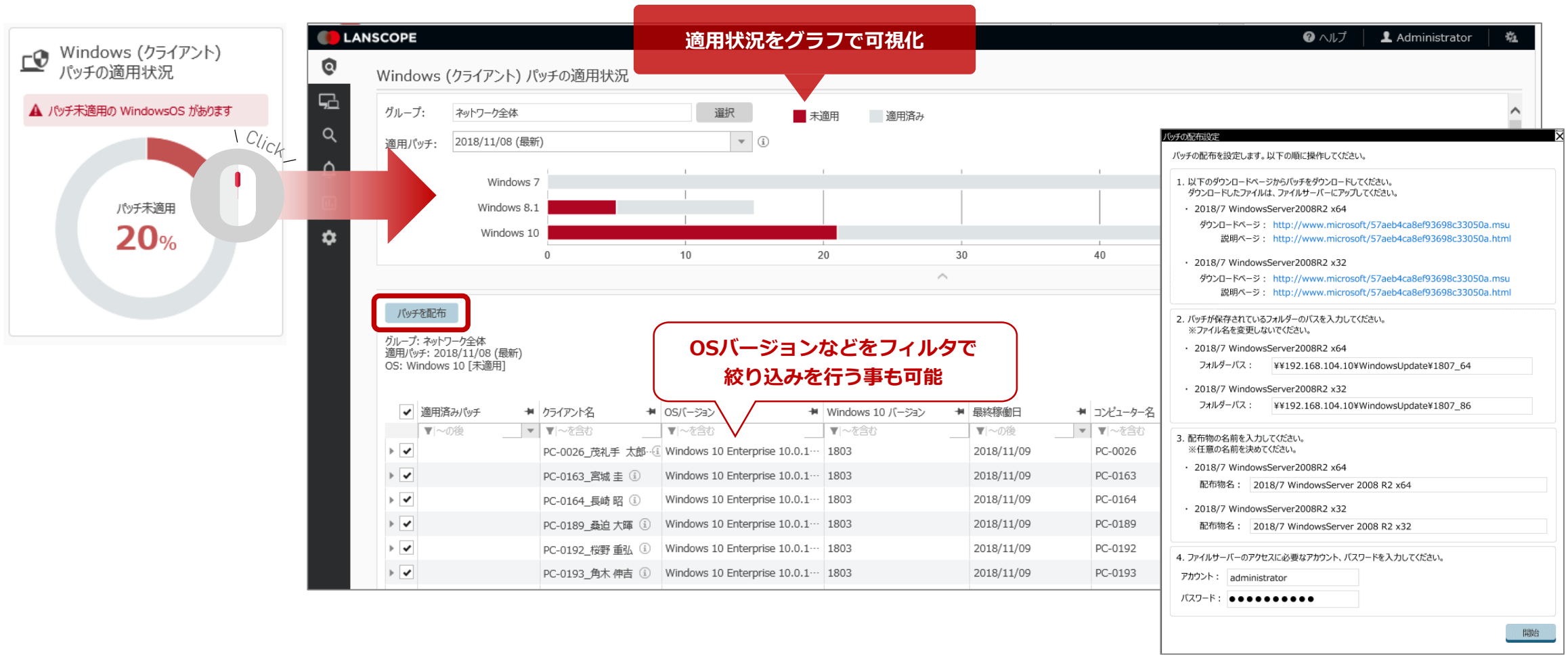
最新の状態でない＝脆弱性がある場合は赤色で表示されるので対策の必要有無をカンタンに判断できます



※ Adobe Reader DC (Continuous) (Adobe Reader旧バージョンも抽出は可能)
Adobe Flash Player (ActiveX, NPAPI)
Java Runtime Environment (8 以下)

パッチの適用情報をグラフ化！未適用者を絞り込みパッチ配布までをワンストップで行えます

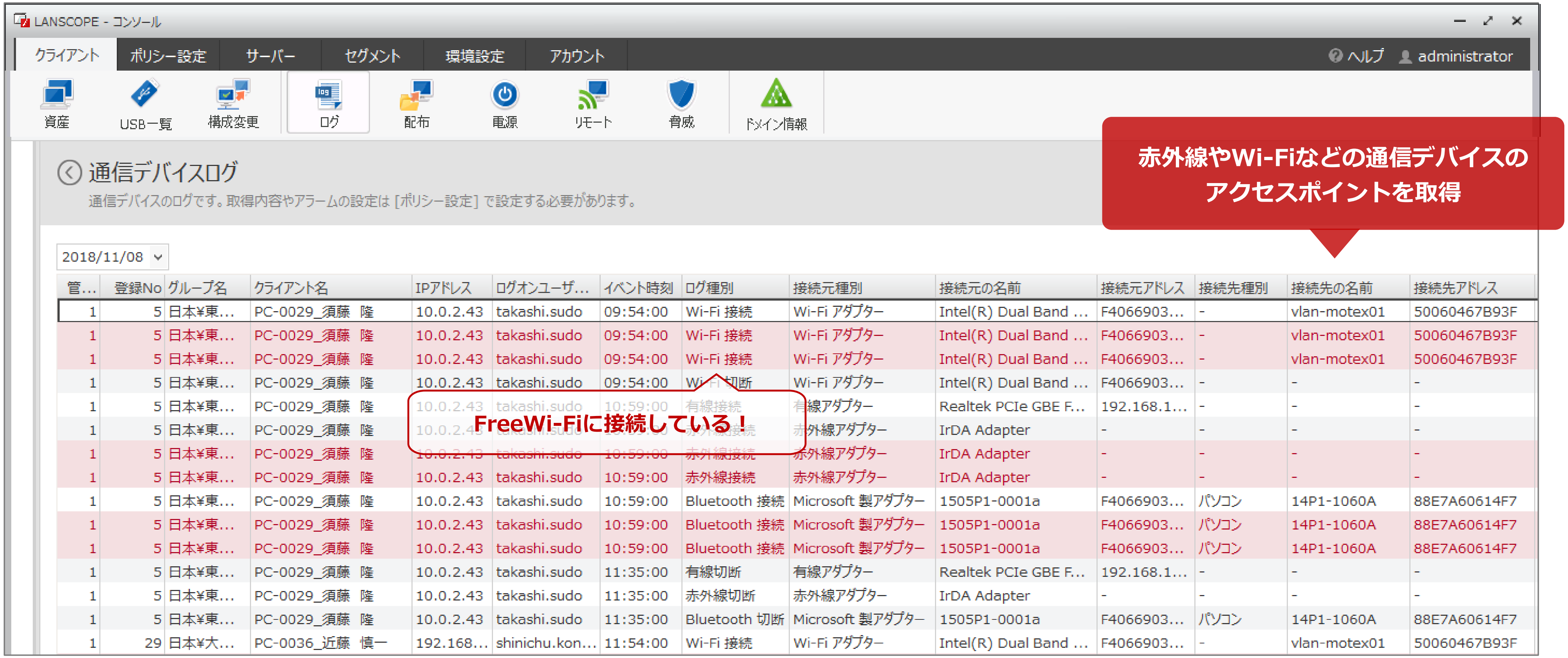
パッチ適用情報をOS毎にグラフ化、パッチ別に確認することも可能です



通信デバイス経由のリスクを対策

リスク急増中！Wi-Fi・Bluetooth・赤外線の接続状況を可視化、危険な接続を制御

管理外のアクセスポイントによるウイルス感染や、通信デバイス経由の情報漏えいなどを察知することが可能です



管…	登録No	グループ名	クライアント名	IPアドレス	ログオンユーザ…	イベント時刻	ログ種別	接続元種別	接続元の名前	接続元アドレス	接続先種別	接続先の名前	接続先アドレス
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	09:54:00	Wi-Fi 接続	Wi-Fi アダプター	Intel(R) Dual Band …	F4066903…	-	vlan-motex01	50060467B93F
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	09:54:00	Wi-Fi 接続	Wi-Fi アダプター	Intel(R) Dual Band …	F4066903…	-	vlan-motex01	50060467B93F
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	09:54:00	Wi-Fi 接続	Wi-Fi アダプター	Intel(R) Dual Band …	F4066903…	-	vlan-motex01	50060467B93F
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	09:54:00	Wi-Fi 切断	Wi-Fi アダプター	Intel(R) Dual Band …	F4066903…	-	-	-
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	10:59:00	有線接続	有線アダプター	Realtek PCIe GBE F…	192.168.1…	-	-	-
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	10:59:00	赤外線接続	赤外線アダプター	IrDA Adapter	-	-	-	-
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	10:59:00	赤外線接続	赤外線アダプター	IrDA Adapter	-	-	-	-
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	10:59:00	赤外線接続	赤外線アダプター	IrDA Adapter	-	-	-	-
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	10:59:00	Bluetooth 接続	Microsoft 製アダプター	1505P1-0001a	F4066903…	パソコン	14P1-1060A	88E7A60614F7
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	10:59:00	Bluetooth 接続	Microsoft 製アダプター	1505P1-0001a	F4066903…	パソコン	14P1-1060A	88E7A60614F7
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	10:59:00	Bluetooth 接続	Microsoft 製アダプター	1505P1-0001a	F4066903…	パソコン	14P1-1060A	88E7A60614F7
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	11:35:00	有線切断	有線アダプター	Realtek PCIe GBE F…	192.168.1…	-	-	-
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	11:35:00	赤外線切断	赤外線アダプター	IrDA Adapter	-	-	-	-
1	5	日本¥東…	PC-0029_須藤　隆	10.0.2.43	takashi.sudo	11:35:00	Bluetooth 切断	Microsoft 製アダプター	1505P1-0001a	F4066903…	パソコン	14P1-1060A	88E7A60614F7
1	29	日本¥大…	PC-0036_近藤　慎一	192.168…	shinichu.kon…	11:54:00	Wi-Fi 接続	Wi-Fi アダプター	Intel(R) Dual Band …	F4066903…	-	vlan-motex01	50060467B93F

未知・亜種のマルウェアも事前検知・隔離！運用工数を最大限に下げたウイルス対策が実現

AIによる予測防御検知を実行。シグニチャレスなので毎日のアップデートは不要で管理者・社員にも負荷をかけません

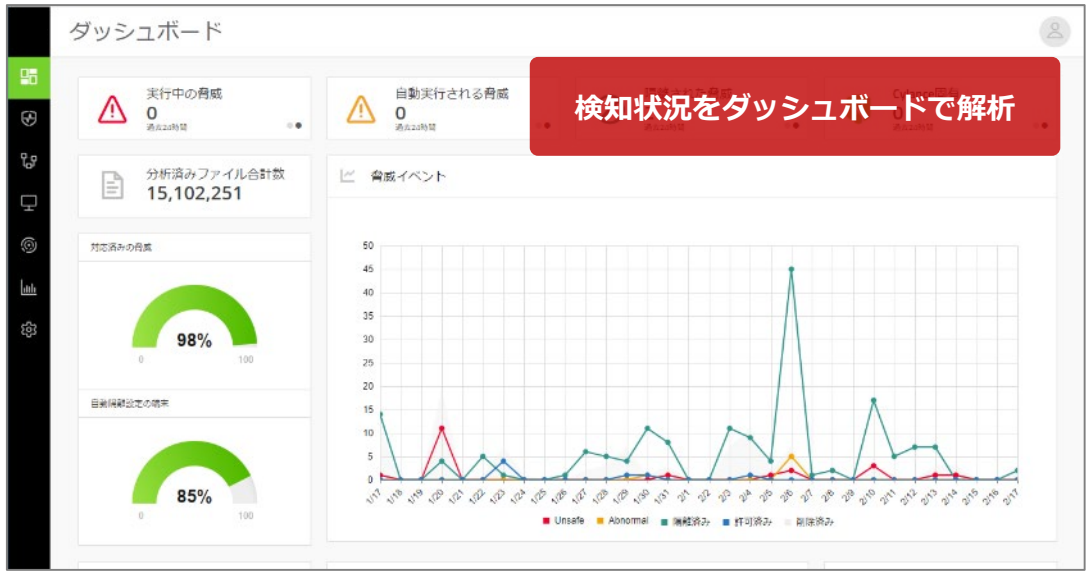
DNAレベルの
マルウェア解析

AIによる自動判断
感染前検知・隔離

シグニチャレス
検知

アップデートは年１
ネットワーク負荷減

非ネット環境下でも
検知・隔離可能



マルウェア検知前後の “人の操作” を把握し、クリックするだけで侵入経路をカンタンに追跡！

専門知識や複雑な検索は不要！なぜ攻撃を受けたのか、原因となった操作をクリックだけで追跡ができます

様々な制御が可能

発見した問題行動に対し、利便性を損なわないセキュリティ対策を実施できます

業務に必要のない操作やリスクのある操作は制御しましょう。ただし利便性を損なわないために、業務影響を考慮した対策を行うことが大切です

不正サイトへの
アクセスを制御

クラウドストレージの
利用を制御

Webメールの
利用を制御

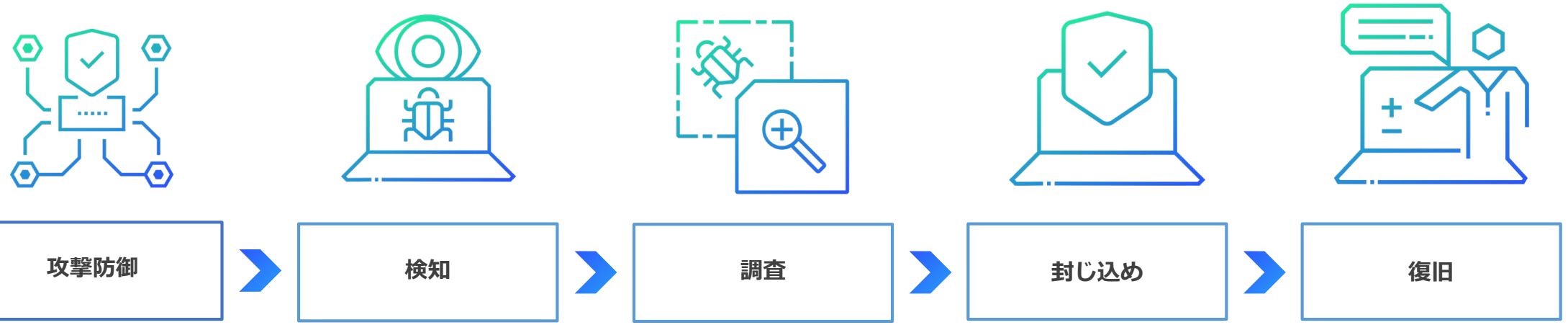
私物のUSBメモリの
利用を制御

FreeWifiなどの危険な
アクセスポイント利用を禁止

本格的に分析したい方におススメのEDR機能「BlackBerry Optics」

検知したマルウェア以外の「端末に潜む脅威」を発見、攻撃の流れを操作を紐づけて可視化

BlackBerry Protectの検知力に加え、調査・封じ込め・復旧まで一連の対応が可能で、負荷の少ないDER機能です



BlackBerry Protectと統合　AIを活用　予防にフォーカス

※BlackBerry Opticsの導入が必要です。詳細はお問合せください

セキュリティ啓蒙

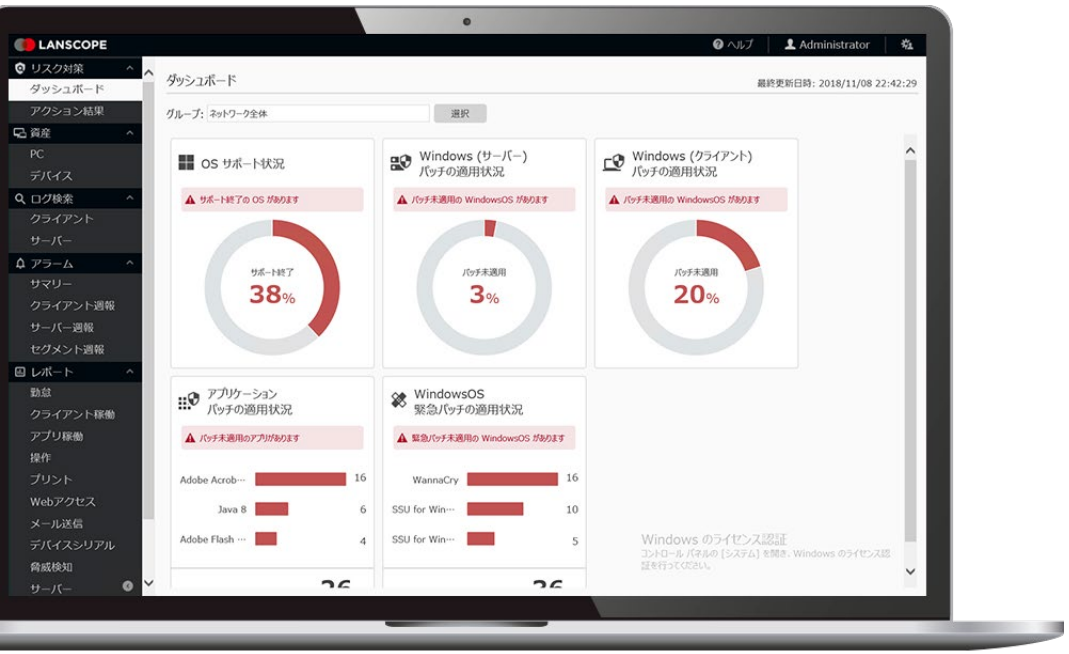
従業員に対するセキュリティ教育で周知・教育・訓練

内部規定等の周知・教育・訓練の実施に最適なのがMOTEXが提供している**「セキュリティブック」**です。全ページWebからPDFを無料ダウンロード可能。また、本書を元にした社内や学校などでセキュリティの研修で活用できる**「講師用資料」**と、その後の復習に活かせる**「テスト」**も無料でPDFを公開しています。

「セキュリティ 7つの習慣・20の事例」PDFデータは、無料でDLできます！ http://www.motex.co.jp/vision/enlightenment_activity/education_book/

LANSCOPEとは

IT資産管理に加え、情報漏えいやマルウェア感染リスクからエンドポイントで守る



統合型エンドポイントマネジメント

LANSCOPE on-premises

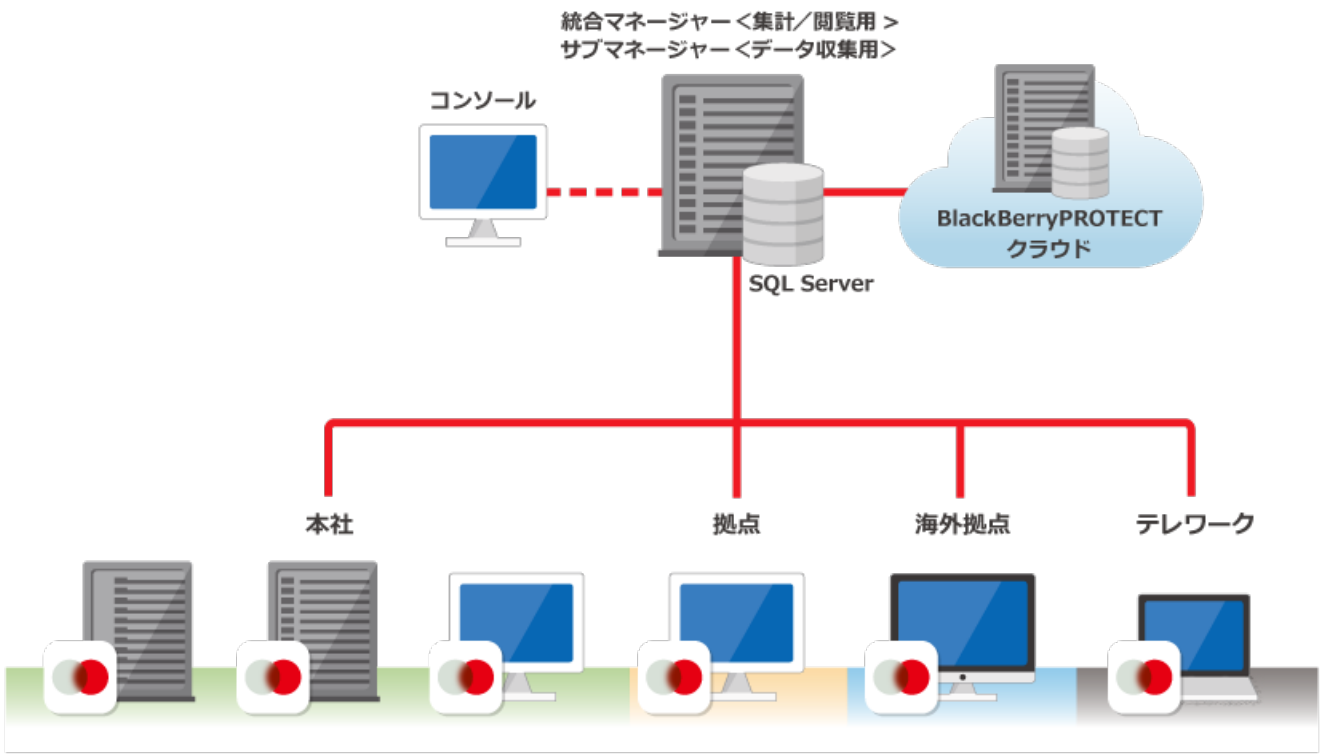
- IT資産管理・内部不正対策・外部脅威対策がワンストップで対応可能
- PC・スマートデバイス・スマホを一元管理
- 国内のみならず海外端末も一元管理、VPN外でも管理が可能
- 必要な機能だけを選択して導入可能

IT資産管理	**操作ログ管理**	**Webアクセス制御**
デバイス制御	**マルウェア対策**	**ﾘﾓｰﾄｺﾝﾄﾛｰﾙ機能**

https://www.lanscope.jp/cat/

エンドポイントに管理モジュールをインストール！通信の暗号化によりインターネット経由でも安全です

Unicode対応を行っており、国内はもちろん海外の端末管理も国内と同じセキュリティレベルで管理が可能です



（IaaS）お客様のクラウド環境に立てる

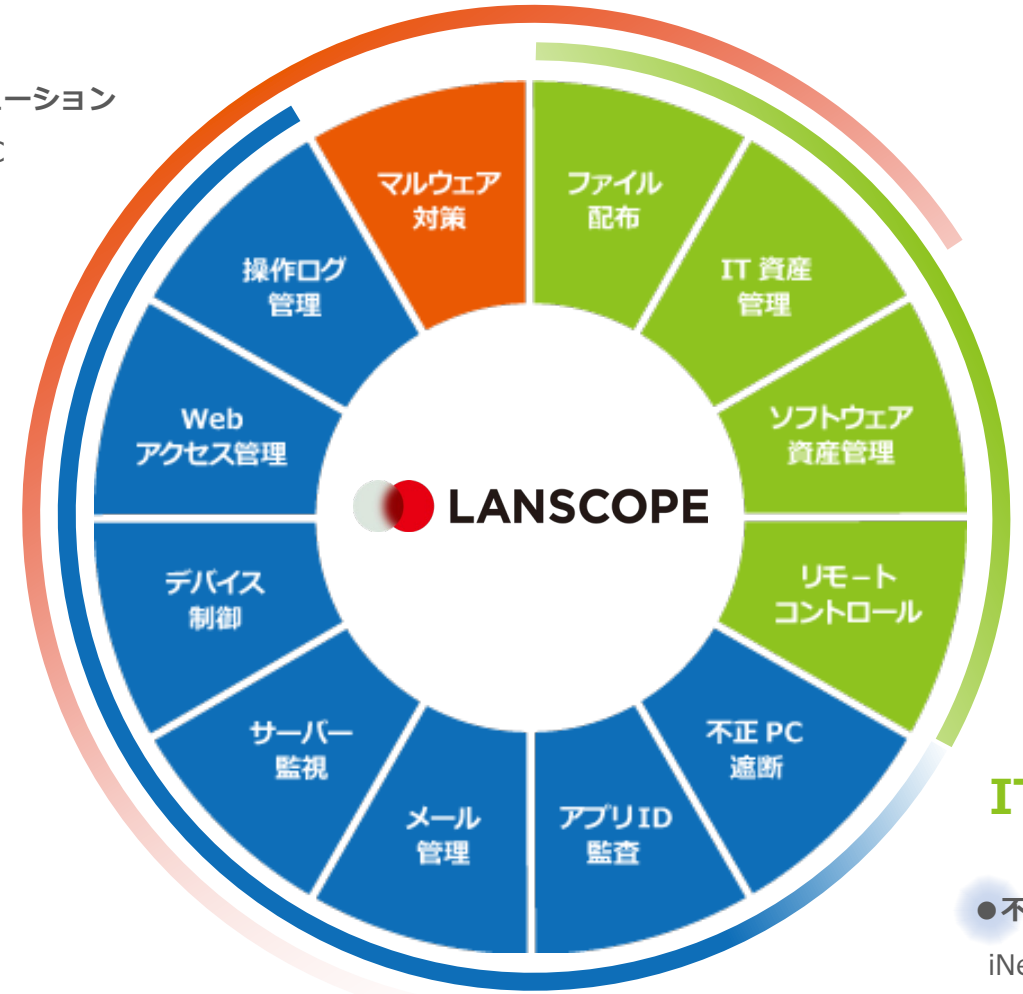
LANSCOPEは各種クラウド基盤に対応しています

IIJ GIO
aws
NIFCLOUD ニフクラ
vmware
Microsoft Azure
NTT Communications Enterprise Cloud

（SaaS）SaaSベンダー提供のサービス利用

インターネットイニシアティブ・オプテージ・
ソフトクリエイト・ディーアイエスソリューション・日本事務器

LANSCOPE は統合型エンドポイント（UEM）です



●情報漏えい対策／セキュリティソリューション

すみずみ君・EKRAN・iDoperationSC
P-Pointer

●統合ログ管理ソリューション

LogRevi・Logstorage

●就業管理ソリューション

勤次郎・勤革時・KING OF TIME・ Xronos
奉行Edge 勤怠管理クラウド

●セキュリティUSBメモリ

アイ・オー・データ機器

●LANSCOPE SaaSソリューション

インターネットイニシアティブ
オプテージ・ソフトクリエイト
ディーアイエスソリューション・日本事務器

アイレット（AWS導入支援ソリューション）

●マシンデータ分析プラットフォーム

Splunk

●バックアップソリューション

AOSBOX

●クラウドベース業務プラットフォーム

ServiceNow

IT資産管理

●不正PC検知ソリューション

iNetSec・L2Blocker・InfoCage・IntraGuardian2+
Secure Enterprise SDN

LANSCOPE 機能一覧

V：バーチャルライセンス（SBC方式シンクライアント管理）対応　　Mac:Mac 端末管理対応

※バーチャルライセンス／ Mac 端末管理には専用ライセンスの購入が必要です。

ライセンス	機能名	区　分	V	Mac	概　要
マネージャーライセンス ※マネージャーライセンス （必須）	レポート	ダッシュボード・レポート			組織の弱い部分を監視し、問題点の自動抽出から対策までをワンストップで実現、グループ別、日付別など様々な切り口でログを集計／グラフ化できます。
		アラーム管理			ルール違反の有無をグループ単位／人単位で把握できます。各種ログを複数条件で組み合わせ、より重要度の高い1つのアラームとして通知できます。
		ログ検索／ファイル追跡			様々な条件で５年分のログを検索。抽出した特定ファイルの流出経路を追跡できます。
	ネットワーク検知	持ち込みPC検知			持ち込みPCなどの不正接続を検知し、リアルタイムに通知します。
		SNMP機器管理/死活監視			SNMP対応機器の情報を収集。稼働状況を確認し、死活監視ができます。
IT資産管理ライセンス	IT資産管理	ハードウェア管理		●	コンピューター名、IP アドレスなどの資産情報を自動取得。プリンター／周辺機器などを、任意で資産登録して管理できます。
		ソフトウェア管理		●	ソフトウェアのインストール情報を自動取得／集計し、許可／不許可を分類できます。
		アプリ稼働ログ管理／制御		●	アプリの稼働情報を取得し、未使用アプリを把握。不正アプリは禁止もできます。
		USB 管理		●	接続されたUSBデバイスを自動検出し、台帳作成や未使用期間の確認ができます。
		電源／省電力管理			指定時刻にPC 電源の強制OFF や、PC省電力設定の一括変更ができます。
		メッセージ・アンケート			管理者からユーザーに対して、メッセージ・アンケートを送信できます。
		ソフトウェア資産管理（SAM）			ソフトウェア辞書を活用し、SAM に必要な台帳を作成。ライセンス違反を把握、また、アップグレード、ダウングレードなどの契約情報も管理できます。
		更新プログラム配布／脆弱性対策			サービスパック、更新プログラムの適用状況の把握。未適用PCに配布できます。
		アプリ配布／自動インストール			アプリの一括配布／インストールができます。また、インストール手順を録画することで、スクリプトを自動生成できます。
		Microsoft Defender連携			検知状況の集中管理・検知情報の管理者メール通知などMicrosoft Defenderの運用管理における課題を解決します。
操作ログ管理ライセンス	操作ログ管理	アプリ稼働ログ管理／制御	●	●	アプリの稼働情報を取得し、未使用アプリを把握。不正アプリは禁止もできます。
		操作ログ管理	●	●	PC 上での画面閲覧（ウィンドウタイトル）やファイル操作を記録できます。
		プリントログ管理	●	●	印刷状況を記録し、ドキュメントやプリンター、PCごとに印刷枚数を集計できます。
		アプリ通信ログ管理	●		通信元／先のIP アドレスやポート番号、アプリのハッシュ値を取得できます。
		通信デバイスログ管理			Wi-Fi ／Bluetooth／赤外線／ 有線の接続を把握し、管理外の接続を検知できます。
		勤怠ログ管理			各クライアントの勤怠情報（業務開始時間、業務終了時間、残業時間など）を閲覧できます。
Webアクセス管理ライセンス	Webアクセス管理	Webアクセスログ管理	●	●	Webサイトの閲覧や書き込み、Webメールやクラウドストレージへのアップロード／ダウンロード操作を記録します。
		Webアクセス制御／ホワイトリスト	●		不正サイトや操作の禁止もできます。またキーワードを指定し、特定のWebサイトのみ閲覧可能にできます。
		クライアントWebフィルタリング（OP）	●		フィルタリングデータベースを用い、カテゴリからWebの閲覧を一括制御できます。
デバイス制御ライセンス	デバイス制御	デバイス制御		●	CD／DVD、フロッピー、USBメモリなどのデバイス種別単位で制御、PCごとに禁止／許可／読み取り専用／一時許可／一時読み取り専用の設定ができます。
		個体識別管理		●	個別デバイスごとに禁止／許可／読み取り専用／一時許可／一時読み取り専用の設定ができます
		接続USB管理		●	社内で利用したUSBデバイスを一覧で確認。未使用期間や最終使用者を把握できます
		デバイス責任者設定			管理者以外に、登録したデバイスの利用を許可できる責任者を設定。責任者は自分のPCから許可／読み取り専用／一時許可／一時読み取り専用の設定ができます。
		通信デバイス制御			Wi-Fi ／ Bluetooth／赤外線通信への接続を制御できます。
メール管理ライセンス	メール管理	送信メールログ管理			Microsoft Outlook送信メールの内容や添付ファイルを記録できます。
アプリID監査ライセンス	アプリID監査	ID監査ログ管理	●		システムへのログイン情報を記録し、なりすましなど不正なID使用を把握できます。
		特権ユーザー管理	●		特権ユーザーによるIDの作成、権限変更などの操作を記録できます。
マルウェア対策ライセンス	マルウェア対策	マルウェア検知		●	AIによる機械学習エンジンにより、未知の脅威をリアルタイムに発見できます。
		マルウェア隔離		●	検知した脅威ファイルをポリシーに応じて隔離できます。
		原因追跡（操作ログ管理）		●	インシデント発生前後の操作を確認することができます。
サーバー監視ライセンス	サーバー監視	ファイルサーバーアクセスログ管理			WindowsやNetAppへのアクセスを記録し、権限のないアクセスを把握できます。
		ファイルサーバー容量管理			フォルダー容量を監視。設定したしきい値を超えると、管理者にメールで通知できます。
		ドメインログオン・ログオフ管理			Active Directoryサーバーを監視し、ドメインへのログオン・ログオフを記録できます。
PC遮断ライセンス	不正PC遮断	持ち込みPC遮断			持ち込みPCなど、セキュリティリスクのあるPC接続を遮断できます。
リモートコントロールライセンス	リモートコントロール	リモートアクセス（ワンタイム型/ 常駐型）		●	PCやサーバーに対し、管理者からリモートで画面操作ができます。
		Web会議			Web上の会議で資料や画像の共有、音声＆ビデオチャットができます。

LANSCOPE 機能一覧

今、必要な機能だけを選んで導入できるので、コストを抑えて導入できます

パッケージ	機　能	
	マネージャーライセンス	レポート／ダッシュボード／アラーム管理／ネットワーク検知
標準パック	IT 資産管理	IT資産管理/SAM／ファイル配布・パッチ適用／Microsoft Defender連携 ※
パック1000	操作ログ管理	アプリ稼働管理・制御／操作ログ・印刷ログ管理
プレミアムパック	Webアクセス管理	Webアクセスログ管理／Webアクセス制御/フィルタ
	デバイス制御	デバイス禁止・読込許可／USB責任者設定
	メール管理	メール送信ログ管理
	アプリID監査	ID使用ログ・特権管理
	マルウェア対策	マルウェア検知･隔離／原因追求
	サーバー監視	サーバーアクセスログ管理／サーバー容量管理
	不正PC遮断	持ち込みPC遮断
	リモートコントロール（REMO-CON）	リモートアクセス／Web会議

選べる購入方法

初めてご購入される方は、マネージャーライセンスが必須

●お得なパックを選ぶ!!

例１　マネージャーライセンス ＋ パック1000

例２　マネージャーライセンス ＋ パック1000 ／ マルウェア対策

●必要な機能を選ぶ!!

例３　マネージャーライセンス ＋ 操作ログ管理 ／ デバイス制御

※Microsoft Defender連携機能は次のいずれかのライセンスを保有さている場合に使用可能です（IT資産管理・操作ログ管理・Webアクセス管理・デバイス制御・アプリID監査・メール管理）

導入に必要な環境

●マネージャー/サブマネージャー／Web コンソールマネージャー

OS	Windows Server 2012、 Windows Server 2012 R2、 Windows Server 2016、 Windows Server 2019
CPU	2.0GHz 以上
メモリ	4GB 以上
HDD空き容量	200GB以上
データベース	SQL Server 2012、SQL Server 2014、SQL Server 2017 SQL Server 2019
Webコンソール（ブラウザ）	Internet Explorer 11 以上、 Google Chrome 69 以上 Mozilla Firefox 62 以上

※100台環境の場合

●エージェント

	Windows	macOS
OS	Windows XP / Windows Vista Windows 7 / Windows 8 Windows 8.1 / Windows 10 Windows Server 2003 Windows Server 2003 R2 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	macOS Big Sur macOS Catalina macOS Mojave macOS High Sierra macOS Sierra

＊マネージャーのハードウェア環境は、クライアント数100台までの推奨環境です。管理する台数や収集するログにより推奨環境が異なります。
＊マネージャーサーバーは、同一OS内に他システムと共存させることも可能ですが専用ハードウェアをご用意いただくことを推奨しています。共存させる場合、問題発生時の切り分けなど、サーバーの分離をお願いする場合があります。
＊データベースは本製品に付属の製品、もしくはお持ちのMicrosoft SQL Serverライセンスが利用できます。
＊500台以上をクラウド環境で管理する場合、本製品に付属のSQL Server(Standard Edition)は利用できません。
＊エージェントの動作環境（CPU、メモリ、HDD空き容量）はOSの推奨システム要件を満たしてください。同居ソフトウェアの使用状況により必要となるシステム要件が変更になる場合があります。
＊クライアントエージェント（MR）は日本語／英語／中国語（簡体字）の海外OSに対応しています。
＊Mac OS X Mountain Lion以前の管理には、LANSCOPE Ver.9.0.0.0のクライアントエージェントを利用する必要があります。
＊対応OSについての詳細は、弊社Webサイト公開のOS対応表をご覧ください。
※Apple M1チップ搭載端末ではMacMRは正常に動作しませんので、MacMRのインストールはお控えください。

LANSCOPE が選ばれる４つの理由

LANSCOPEの優位点・魅力

導入社数20,000社以上！トップシェアのIT資産管理ツール

導入後も95%以上の方に使い続けていただける「製品力」と「サポート力」が強みです

シリーズ導入実績20,000社

長期継続利用

ITreviewリーダー

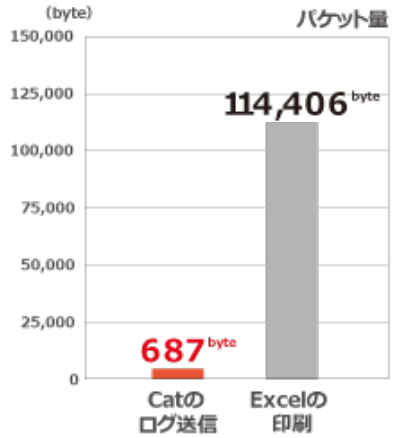
10期連続獲得

ネットワーク負荷・クライアント負荷の軽さや保存容量の少なさが評価

1990年創立からの実績・ノウハウで実現！PCのスペックが低く、ネットワークも細い時代から開発を続けてきました

●ネットワーク負荷の軽さ

LANSCOPEのログ送信時のネットワーク負荷は、Excel A4ドキュメントを1枚印刷した時の160分の1です。ネットワークアナライザを開発していた技術があるから実現できた圧倒的な性能です。

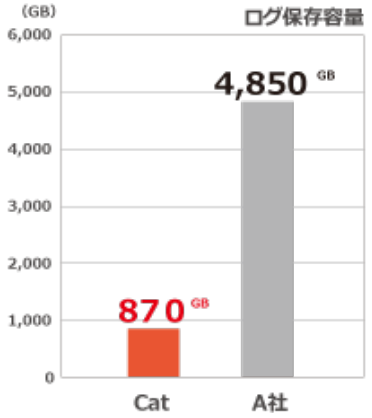


●クライアント負荷の軽さ

LANSCOPEは他社製品の常駐エージェントと比べて、XenApp™サーバーに40ユーザーがアクセスした時のCPU負荷を3分の1に抑えています。

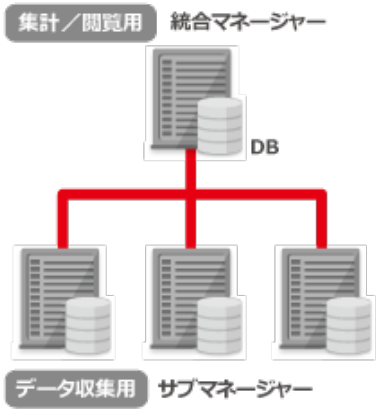
●ログ保存容量の少なさ

LANSCOPEは人が操作した内容を判別する仕組みで、必要ない大量のシステムログなどをフィルタします。他社製品の約5分の1までログ保存容量を抑え、HDDを圧迫しません。



●システムの負荷分散

LANSCOPEは、サーバーを集計／閲覧用とデータ収集用に分けることでシステムの負荷を分散しています。大規模環境でも運用可能な構成で、4万台のPCを管理している実績があります。

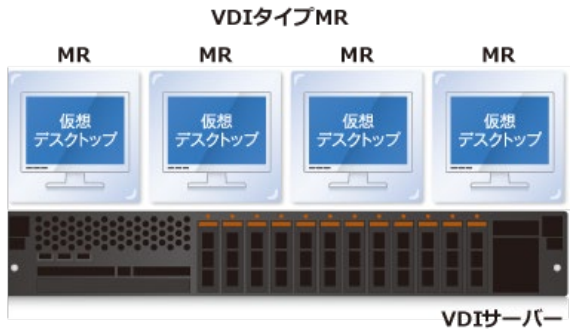


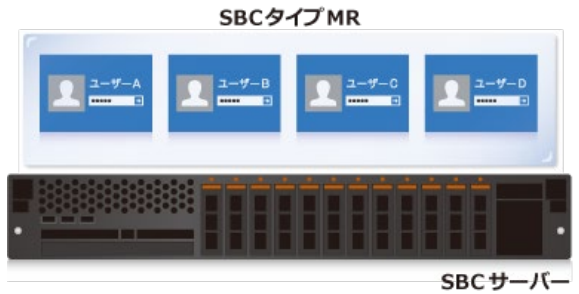
LANSCOPEは環境対応も幅広く、様々な環境にも対応が可能です。

様々なワークスタイルに合わせた環境のセキュリティ対策にご利用いただけます！海外でも国内同様のセキュリティレベルで対策が可能です

シンクライアント

AWS／CITRIX／VMWareに対応





グローバル対応

Windows（Unicode対応）

日本語以外に英語／中国語（簡体字）のOS も正式にサポート

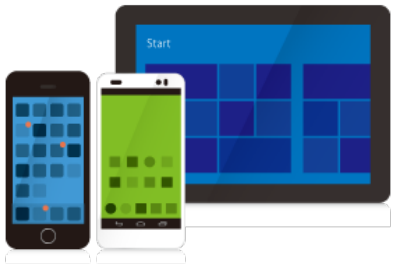
Mac（Unicode対応）

Mac端末管理の独自機能として
フォント管理機能も実装

スマートデバイス管理

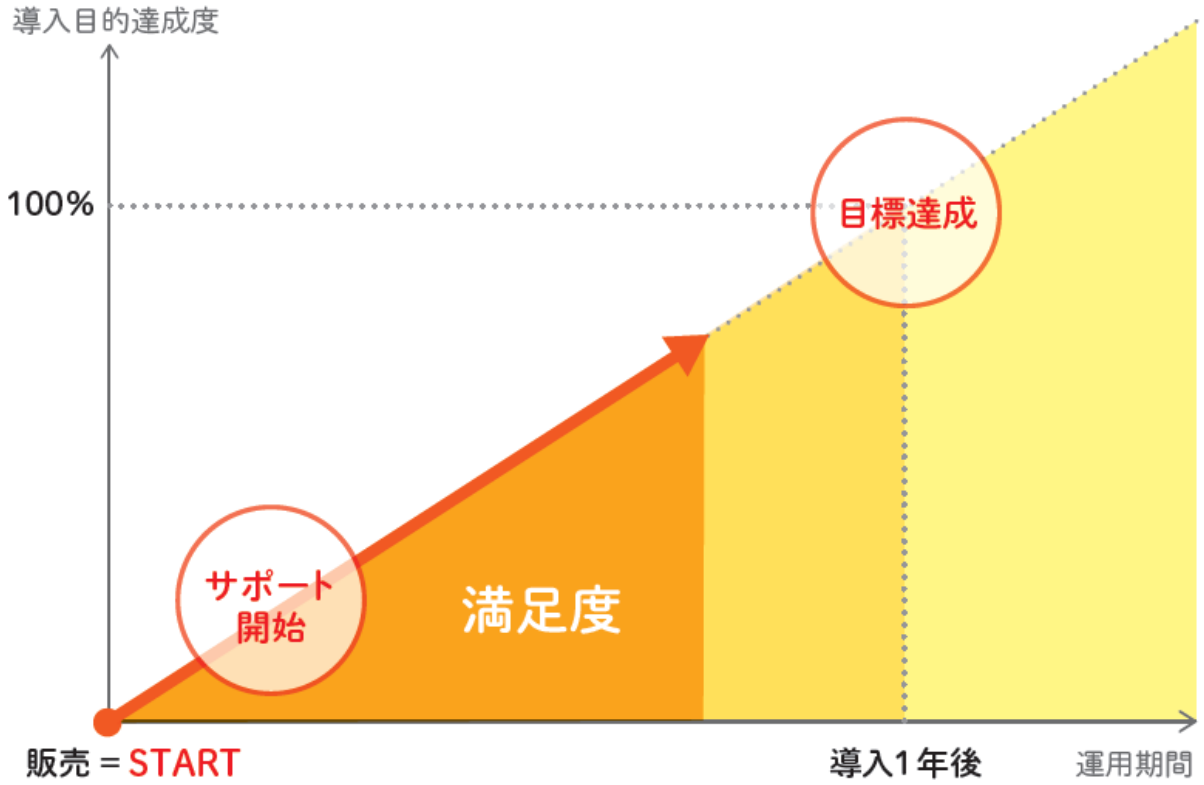
iOS/iPad
Android
Windows
Mac

紛失／盗難対策から現在位置や
移動履歴まで管理できます。



ご購入頂いてからがスタート！定期フォローや様々な運用支援の体制をご用意

購入して頂いたお客さま１社１社に専任スタッフが運用フォロー！



定期フォローサービス

導入後1年間、定期的にフォロー担当者からお電話させていただきます。お客様の導入目的を実現するために専用のWebナビゲーションコンテンツを使いながらサポートいたします。

引き継ぎフォローサービス

LANSCOPEのご担当者様情報の変更・追加があったユーザー様に、オリジナルキットを用い、製品の使い方などの運用支援を行います。

LANSCOPE Portal（保守契約ユーザー様専用サイト）

LANSCOPEの最新プログラムや運用の為の各種資料、MOTEXからの最新情報やよくあるご質問（FAQ）の閲覧、製品の基礎から活用方法までが簡単にわかる「猫ナビ」がご利用できます。

各種ユーザー様イベント開催

基調講演やLANSCOPEの導入事例など、ユーザー様の運用の参考にしていただけるような様々なユーザー様イベントを開催しています。

1ヶ月間 無料体験キャンペーン中

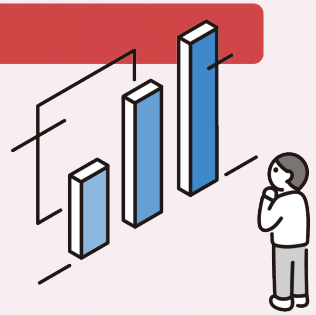
体験版
お試し限定

今だけ
レポートサービス
実施中

インストールから31日間、LANSCOPEオンプレミス版の全機能利用可能な体験版をご用意しています。
体験版は**お手軽な「クラウド環境」**と**「オンプレ版」**の2種類をご用意。
サーバーの用意不要で最大50台まで管理いただけますので、是非この機会にお気軽にお試しください。
さらに今だけレポート提供、加えて本格的に導入検討方にはメーカーSEによるレポートを用いた運用
レクチャーサポートを実施中です（※申込フォームにてエントリーしてください）

＋ レポートサービス

５台以上に展開・検証の方には
体験版終了後にレポート提供



＋ レクチャーサービス

100L以上で導入検討されている方は
運用フォロー×レポート提供

https://go.pardot.com/l/320351/2017-06-20/c4vz?re

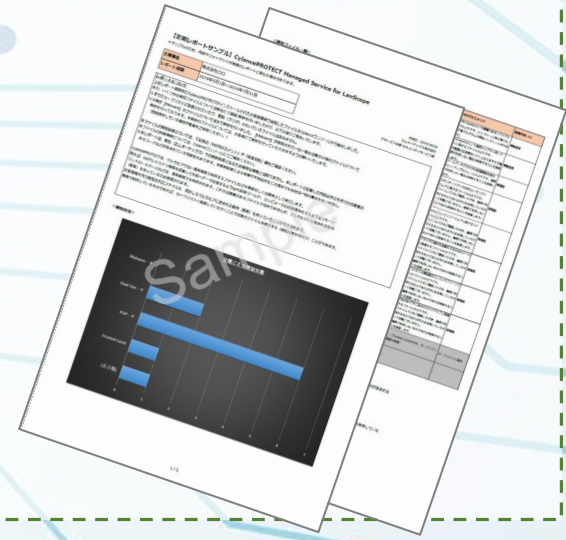
BlackBerry Protect

AIアンチウイルス無料体験実施中

～BlackBerry Protectを気軽に使ってみよう～

最新AIを活用した新技術で超高精度の検知率を誇る「BlackBerry Protect」を**1ヶ月無料**で**何台でも体験**できるキャンペーンがスタートしました。実際に自社のPCにBlackBerry Protectをインストールし、コンソールの操作方法や検知力の高さを体験いただけます。

体験終了後、エムオーテックスにて**検知結果のサマリーレポートをご提供**します。
AIを活用した最新鋭のアンチウイルス製品を、この機会にお気軽にご体験ください！



●お申し込みはこちらから

https://go.motex.co.jp/l/320351/2019-06-27/2fv6jr?tech06

本資料は2022年4月施行の「令和２年 改正個人情報保護法について」（2021年7月時点の情報）に基づいて作成しています
あくまで抜粋・まとめ版となりますので、正式版もご参照いただくことを推奨します
個人情報保護委員会：https://www.ppc.go.jp/personalinfo/

エムオーテックス製品に関する問い合わせは下記にて受付いたします
sales@motex.co.jp