LANSCOPE

BlackBerry. Protect

地方公共団体における情報セキュリティポリシーに関するガイドライン

本資料は令和2年12月28日に公開された 総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和2年12月版）」に基づいて作成しています。

地方公共団体における情報セキュリティポリシーに関するガイドライン

■地方公共団体における情報セキュリティポリシーに関するガイドラインとは

総務省が策定するガイドラインで、地方公共団体が、各組織の情報セキュリティを確保するための方針・体制・対策等を包括的にまとめる「情報セキュリティポリシー」を定めるための参考として示すものです。地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産を守るにあたって自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものとされています。

2020年12月28日に「令和2年12月版」が公表され、「クラウド・バイ・デフォルト原則」、行政手続のオンライン化、働き方改革、サイバー攻撃の増加といった新たな時代の要請や「三層の対策」の課題を踏まえて2020年5月22日に取りまとめられた「自治体情報セキュリティ対策の見直しについて」をベースにガイドラインの改訂が行われています。

総務省
MIC Ministry of Internal Affairs and Communications

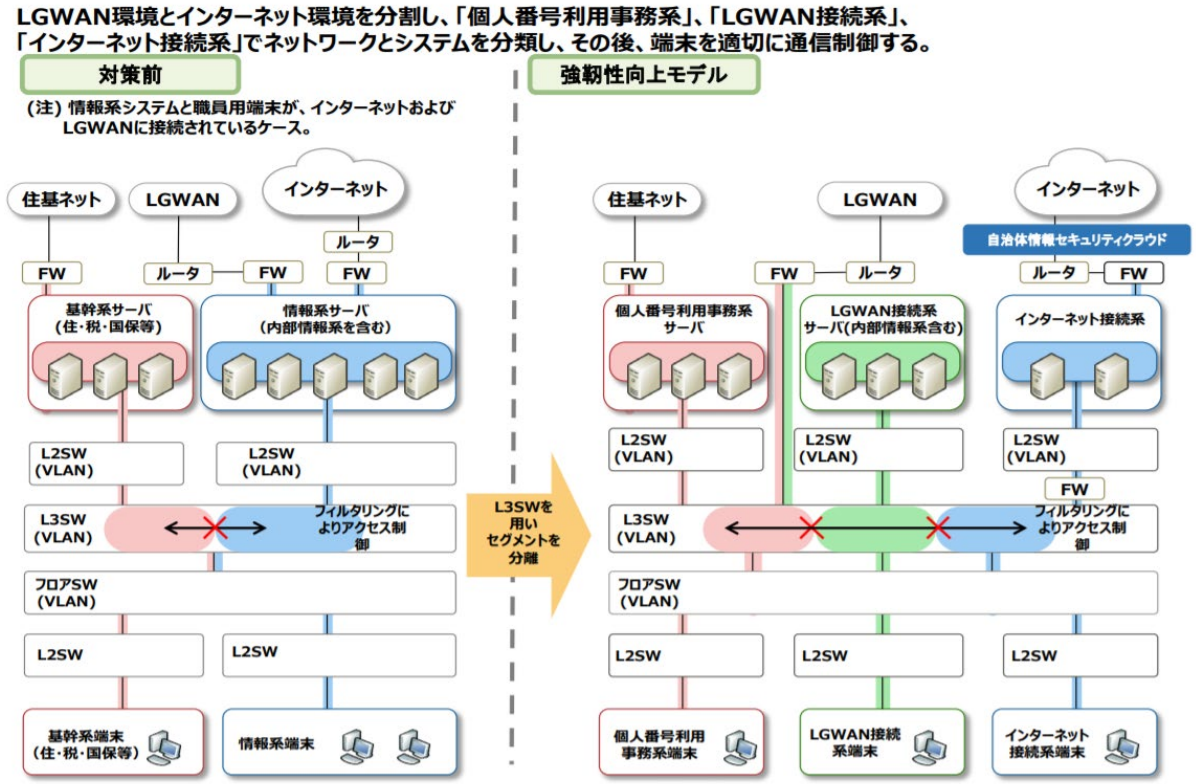
ガイドラインのポイント

- 情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化すること
- 情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策をすること
- 地方公共団体は、自らの情報セキュリティを確保するとともに、地域全体の情報セキュリティの基盤を強化すること
- 地域における広報啓発や注意喚起、官民の連携・協力等に　積極的に貢献すること

ガイドラインを満たすセキュアな環境構築

■用途に合わせてネットワークを分離することで、リスクヘッジができるネットワーク構成を「αモデル」と定義

すべての地方公共団体において、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが求められています。複雑、巧妙化するサイバー攻撃の脅威に対応するため、情報システム全体の強靭性の向上として、ネットワークを「マイナンバー利用事務系」「LGWAN接続系」「インターネット接続系」の3つに分離し、それぞれの領域との間での通信を制御する「三層の対策」が求められています。 2020年12月9日に公開された改定案では、従来の「三層の対策」のネットワーク構成を、改めて「αモデル」と定義し、新たに「βモデル」「β'モデル」を提示しました。



出典：地方公共団体における情報セキュリティポリシーに関するガイドライン (令和2年12月版)
図表 16 強靭性向上モデルにおけるネットワーク再構成の一つのイメージ

αモデル構築のポイント

- 情報システム全体に対し、三段階の対策を講じることとされ、ネットワーク分離環境での強固なセキュリティ対策が求められています。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにする。

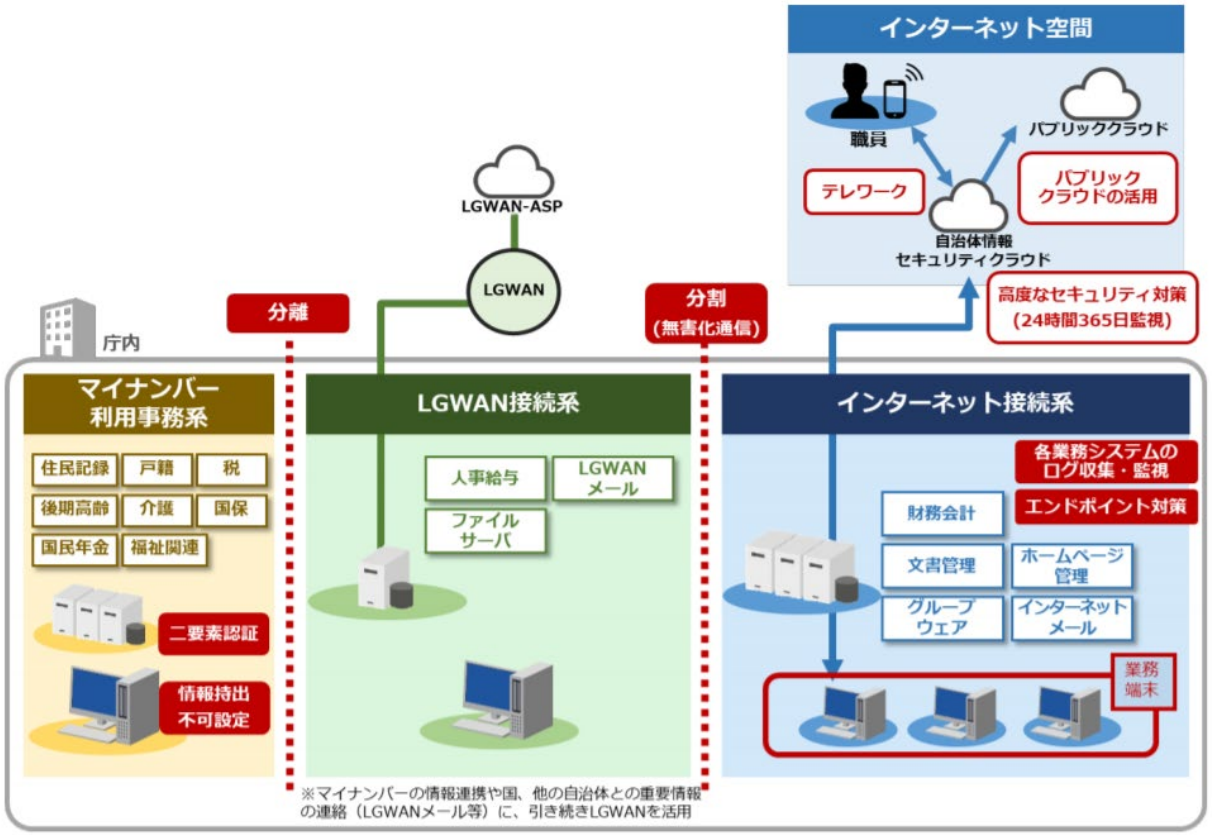
②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

ガイドラインを満たすセキュアな環境構築

■「αモデル」に対して、より効率性・利便性を高めた「βモデル」「β'モデル」が選択可能に

「βモデル」では、業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末を配置することができます。さらに「β'モデル」 では、入札情報や職員の情報などの機密情報もインターネット接続系に配置することができます。一方で「αモデル」の場合と比較してより強固なセキュリティ対策を実施し、さらに外部監査を定期的に実施し、監査報告書の提出が必要となります。セキュリティ対策の強化としては、未知の不正プログラム対策として専門家による監視サービスの活用や、EDR（Endpoint Detection and Response）と呼ばれる異常な挙動の監視・検出・隔離、職員への訓練の実施などが求められます。



出典：地方公共団体における情報セキュリティポリシーに関するガイドライン (令和2年12月版)
図表 23 β'モデルイメージ図

β、β'モデル構築のポイント

●βモデルを採用する場合

インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産をLGWAN接続系に配分することができる。

●β'モデルを採用する場合

インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置することができる。

両モデルとも必要な情報セキュリティ対策※を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならないとされています。

※必須とされるセキュリティ対策の詳細は次ページをご参照ください

【参考】β、β'モデルで必須とされるセキュリティ対策の強化

対策区分	セキュリティ対策	概要	βモデル	β'モデル
技術的対策	無害化処理	ファイルからテキスト情報のみ抽出、ウイルススキャンなどの手法により危険因子がないことを確認したうえでLGWAN接続系にインターネット接続系からファイルを取り込む。	必須	必須
	LGWAN接続系の画面転送	インターネット接続系の業務端末からLGWAN接続系のサーバーや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。LGWAN接続系からインターネット接続系へのデータ転送は禁止とする。ただし、業務で必要となるデータ転送については、中継サーバーやファイアウォール等を設置し、通信先を限定することで可能とする。	必須	必須
	未知の不正プログラム対策	従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活用を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。	必須	必須
	業務システムのログ管理	インシデントの徴候検知や、インシデント発生後の調査に使用するため、業務システムのログの収集、分析、補完を実施する。	必須	必須
	情報資産単位でのアクセス制御	情報資産の機密レベルに応じて業務システム単位でのアクセス制御を行う。文書を管理するサーバー等は課室単位でのアクセス制御を必須とし、係単位でのアクセス制御は推奨とする。	ー	必須
	脆弱性管理	OSやソフトウェアのバージョンなどをもれなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの税者k末井を狙った攻撃に迅速に対応する。	必須	必須
組織的・人的対策	セキュリティの継続的な検知・モニタリング体制の整備	標的型攻撃訓練や研修等の職員等の受講状況や結果を確認し、セキュリティ対策の浸透状況や効果を測定する。測定した結果をもとに改善につなげていく。	ー	必須
	組織的なセキュリティ対策基準の順守	必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。	必須	必須
	住民に関する情報をインターネット接続系に保存させない規定の整備	住民の名簿など、住民の個人情報をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。	必須	必須
	情報セキュリティ研修、標的型攻撃訓練、セキュリティインシデント訓練の受講	職員等は情報セキュリティ研修、標的型攻撃訓練を年1回以上受講する。情報システム管理者、情報システム担当者はセキュリティインシデントが発生した場合の訓練を年1回以上受講する。	ー	必須

▲地方公共団体における情報セキュリティポリシーに関するガイドライン (令和2年12月版)をもとにMOTEX作成

LANSCOPEシリーズで実現する地方公共団体における情報セキュリティ対策

LANSCOPE／BlackBerry Protect

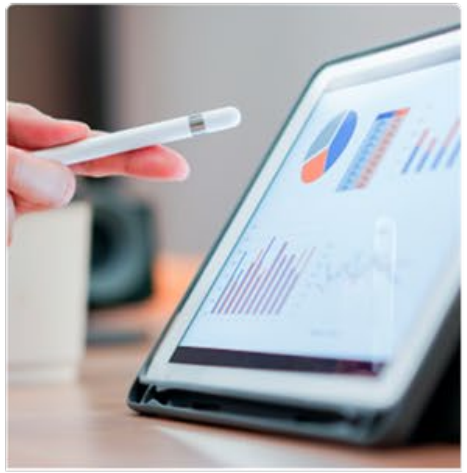
安全と生産性の両立を支援するLANSCOPEシリーズ

■LANSCOPEシリーズ は、α、β、β'のすべての環境のIT活用とセキュリティ強化をご支援します

エムオーテックスは、企業・組織が保有するPC・モバイルデバイスを統合管理する「LANSCOPEシリーズ」をご提供しています。LANSCOPEシリーズの開発コンセプトは「Secure Productivity（安全と生産性の両立）」です。安全か、生産性かの二者択一ではなく、両立することを目指して製品・サービス開発に取り組んでいます。エムオーテックスは、α、β、β'のいずれのモデルを選択される自治体様でも、安全と生産性の両立を実現できるよう、IT活用とセキュリティ強化をご支援いたします。

モバイル管理

IT 資産管理



操作ログ管理

情報漏えい対策

外部脅威対策

LANSCOPE cloud

LANSCOPE on-premises

BlackBerry Protect

LANSCOPEシリーズ で実現する地方公共団体における情報セキュリティポリシー対策

情報セキュリティ対策基準			LANSCOPEシリーズ対応範囲	対応製品
3.情報システム全体の強靭性の向上		(1)マイナンバー利用事務系 ② 情報のアクセス及び持ち出しにおける対策	デバイス制御 利用媒体管理	LANSCOPE on-premises
		(2)LGWAN接続系 ① LGWAN接続系とインターネット接続系の分割	マルウェア対策 (ディスコネクトモード)	BlackBerry Protect
			EDR・ふるまい検知	BlackBerry Optics
		(3) インターネット接続系 βモデル、β'における必須のセキュリティ対策	リモートアクセス時のログ管理	LANSCOPE on-premises
			未知の不正プログラム対策	BlackBerry Protect
4.物理的セキュリティ	4.4. 職員等の利用する端末や電磁的記録媒体等の管理	⑥ モバイル端末のセキュリティ	モバイル管理 リモートワイプ	LANSCOPE cloud
5.人的セキュリティ	5.1. 職員等の遵守事項	(1)職員等の遵守事項 ④ 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用	不正PC検知・遮断	LANSCOPE on-premises
6.技術的セキュリティ	6.1. コンピュータ及びネットワークの管理	(6)ログの取得等	ログ管理	LANSCOPE on-premises
		(15)電子メールの利用制限	Webアクセス管理	LANSCOPE on-premises
		(17)無許可ソフトウェアの導入等の禁止	アプリ管理	LANSCOPE on-premises
		(19)無許可でのネットワーク接続の禁止	不正PC検知・遮断	LANSCOPE on-premises
		(20)業務以外の目的でのウェブ閲覧の禁止	Webアクセス管理	LANSCOPE on-premises
	6.4. 不正プログラム対策	(1)統括情報セキュリティ責任者の措置事項	マルウェア対策 資産管理	BlackBerry Protect
	6.6. セキュリティ情報の収集	(1)セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等	ダッシュボード機能	LANSCOPE on-premises

LANSCOPE on-premises

(1) マイナンバー利用事務系

②情報のアクセス及び持ち出しにおける対策

(イ)情報の持ち出し不可設定

原則として、USBメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

電磁記録媒体による端末からの情報持ち出しを行う場合は次の手段により実施しなければならない。

・端末には利用許可された媒体のみ接続可能とすること。

・利用媒体は、全て管理し利用履歴を残せること。

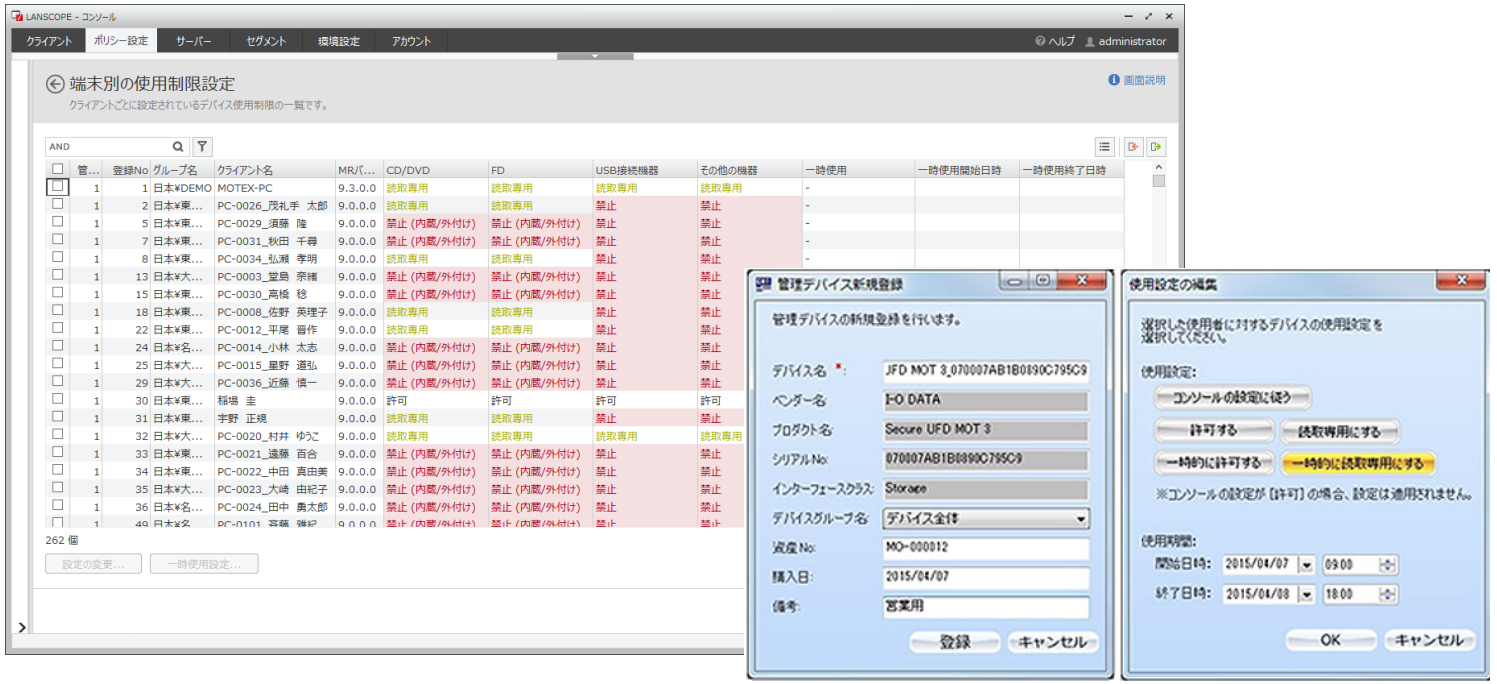
デバイス制御

電磁的記録媒体の利用を制御（禁止）できます

社内のデバイスにおける一元管理・利用制御が可能。利用許可されていないデバイスが接続されると、ユーザーに禁止通知し、不正利用を抑制できます。

また、PCごとデバイスごとの詳細な条件で限定的にデバイス利用が許可できるため、現場に即した運用が可能です。

また、管理PCに接続されたUSBを一覧で表示可能です。



BlackBerry Protect

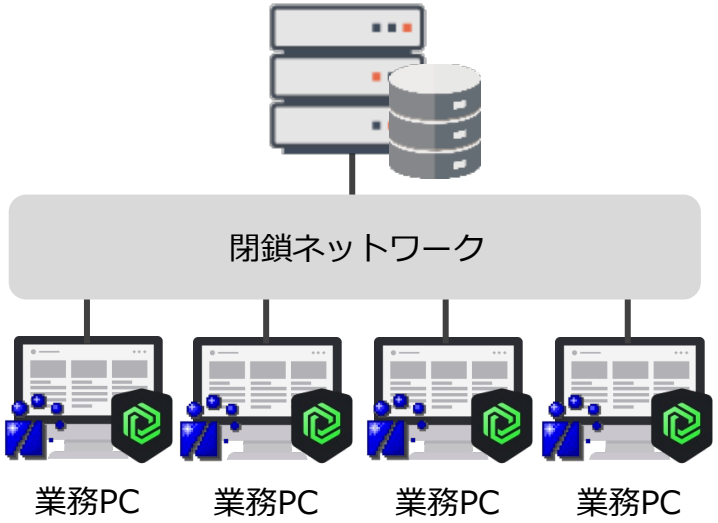
（2）LGWAN接続系
①LGWAN接続系とインターネット接続系の分割
LGWAN接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。

（4）その他のセキュリティ対策
③修正プログラム及びパターンファイルの更新
マイナンバー利用事務系及びLGWAN接続系では、ウイルス対策ソフトのパターンファイルの更新等においても、インターネット接続して利用してはならない。

閉鎖ネットワークのマルウェア対策

クローズなネットワーク分離環境においてもオンプレミスで統合管理。管理負担も低減

インターネット非接続環境でも、オンプレミスの管理サーバーでマルウェア検知状況の確認やポリシー設定、クライアントプログラムの一括アップデートが可能です。
また、定義ファイルを利用しない独自のマルウェア検知手法のため、クライアントプログラムの更新頻度は半年に1度程度。管理者の更新作業の負担を大幅に削減できるだけでなく、ユーザー側もストレスなく利用できます。



オフラインも統合管理

インターネット非接続環境の端末でも、管理コンソールでマルウェア検知状況の把握、遠隔での一括アップデートの操作が可能です。

更新は半年に1回

シグニチャレスの独自のマルウェア検知手法のため、更新は半年に1回程度。2年以上前の検知エンジンで最新のマルウェアを検知できた実績があります。

BlackBerry Optics

（２）LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

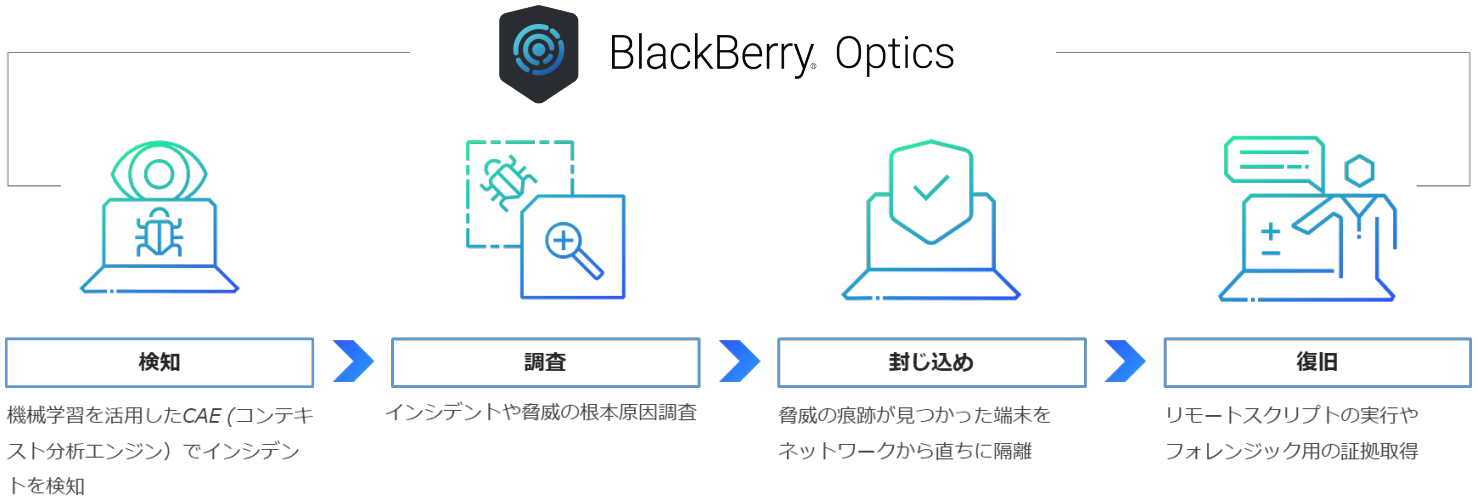
（ウ）危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

EDR・ふるまい検知

AIを活用したEDRでインシデントの発生を未然に防ぎます

予防にフォーカスしたEDRで、AIによる検知から、調査、封じ込め、復旧までの一連の対応を実現します。

「攻撃の可能性がある動作」をあらかじめルールとして設定することで、リモートユーザーのログオフやイベントログへの記録、ユーザーへの通知などを行い、インシデントの発生を未然に防ぎます。



LANSCOPE on-premises

(3) インターネット接続系
【βモデルのシステム構成について】

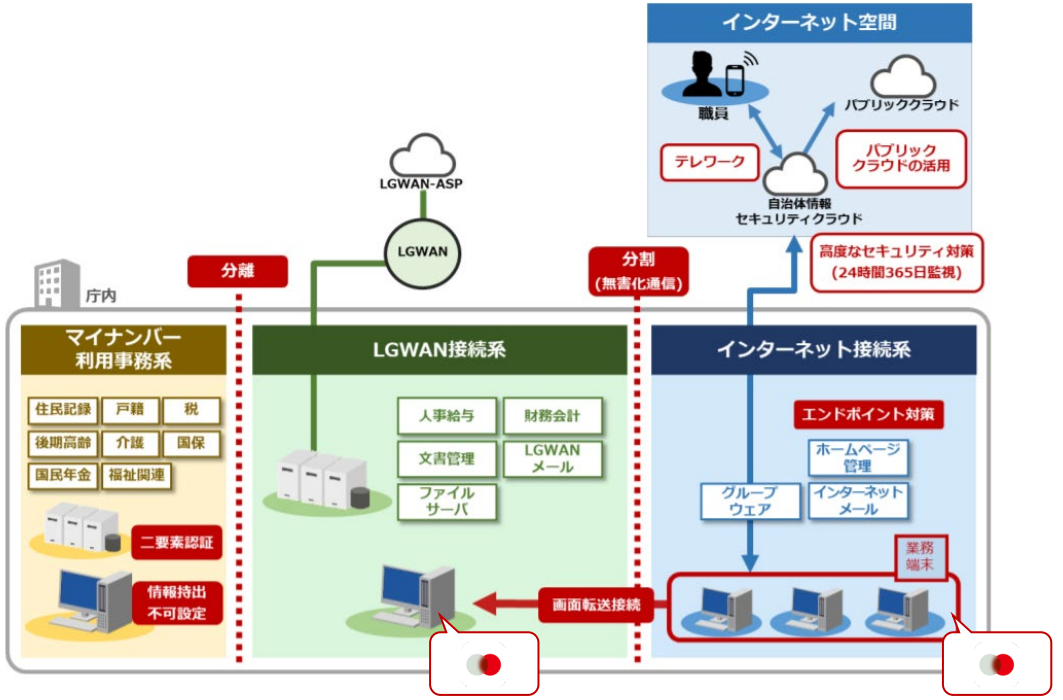
本モデルは、業務システムを LGWAN 接続系に残しつつ、業務端末及びグループウェア等をインターネット接続系に配置し、画面転送により LGWAN 接続系業務システムを利用できるようにしたモデルである。

ログ管理

リモートアクセスをする側・される側の双方のPC操作を記録できます

パソコンの操作履歴をログ化し収集可能です。Bモデルではインターネット接続系の端末からLGWAN接続系の端末へリモートアクセスをして業務することとされています。

リモート操作をする側、される側の双方のPCにLANSCOPEのクライアントプログラムをインストールすることで、もれなくPC操作ログ管理が可能です。



出典：地方公共団体における情報セキュリティポリシーに関するガイドライン（令和2年12月版） 図表 21 β モデルイメージ図

BlackBerry Protect

(3) インターネット接続系
【βモデル、β'における必須のセキュリティ対策について】

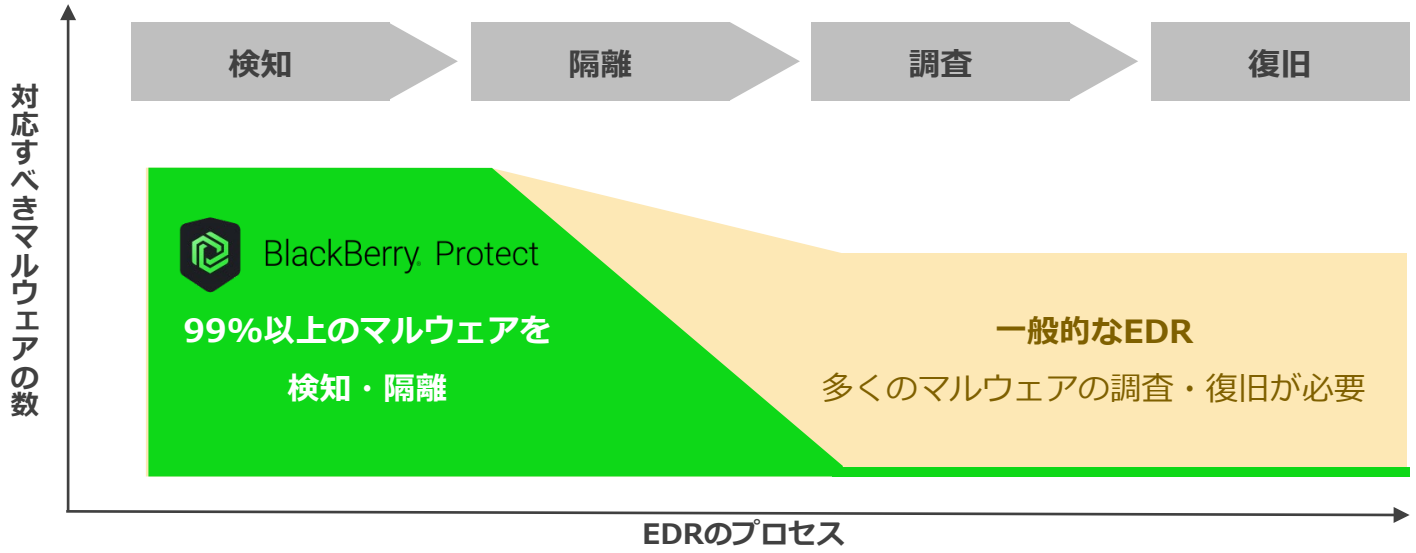
＜未知の不正プログラム対策＞
従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活用を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。

未知の不正プログラム対策

強力なアンチウイルス機能付きEDRで負担の少ないEDR運用を実現できます

BlackBerry ProtectのEDRは、亜種・変異型のマルウェアも99%以上※検知できる、検知率の高さが特徴です。
EDRのプロセスは、検知・隔離・調査・復旧の4つのステップがありますが、検知・隔離の部分で対処すべき数が多ければ多いほど、調査や復旧にかかる負担が小さくなります。EDRは、検知率の高さを重視して製品を選定しましょう。

※2018 NSS Labs Advanced Endpoint Protection Test結果より



LANSCOPE cloud

4.4　職員等の利用する端末や電磁的記録媒体等の管理

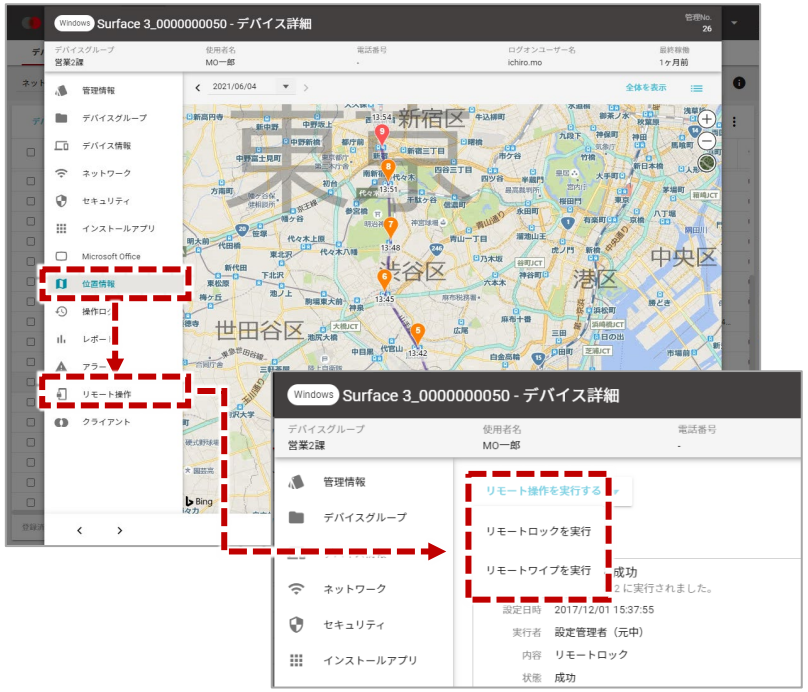
⑥モバイル端末のセキュリティ
モバイル端末を庁外で業務利用する場合は、端末の紛失・盗難対策として、普段からパスワードによる端末ロックを設定しておくことが必要である。
また、紛失・盗難に遭った際は、遠隔消去(リモートワイプ)や自己消去機能により、モバイル端末内のデータを消去する対策も有効である。

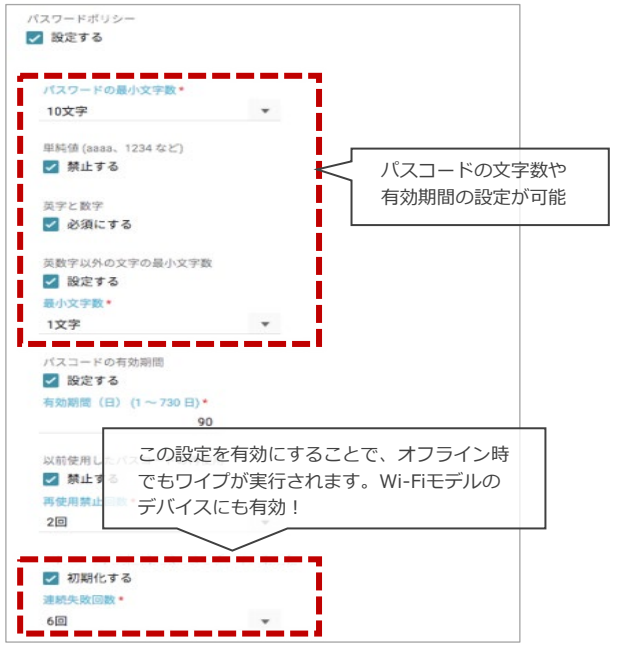
モバイル管理

万が一の紛失に備えて、事前・事後対策ができます

万が一、紛失が発生した場合はデバイスの位置情報を確認し、発見の手がかりにすることが出来ます。見つからない場合は、リモートロック・ワイプを実行し情報漏えいを防ぎます。

事前の対策としてパスワードポリシーを設定することで悪意ある拾得者への対策ができます。





LANSCOPE on-premises

5.1　職員等の遵守事項

(1)職員等の遵守事項

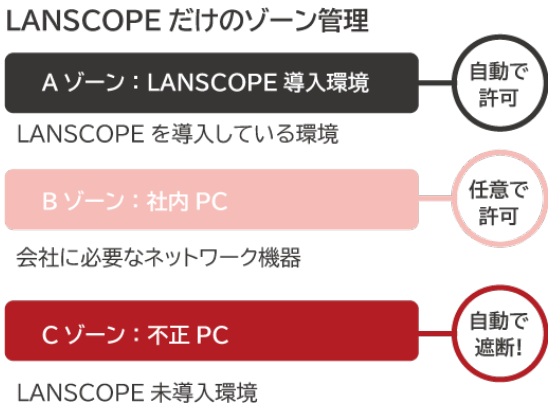
④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

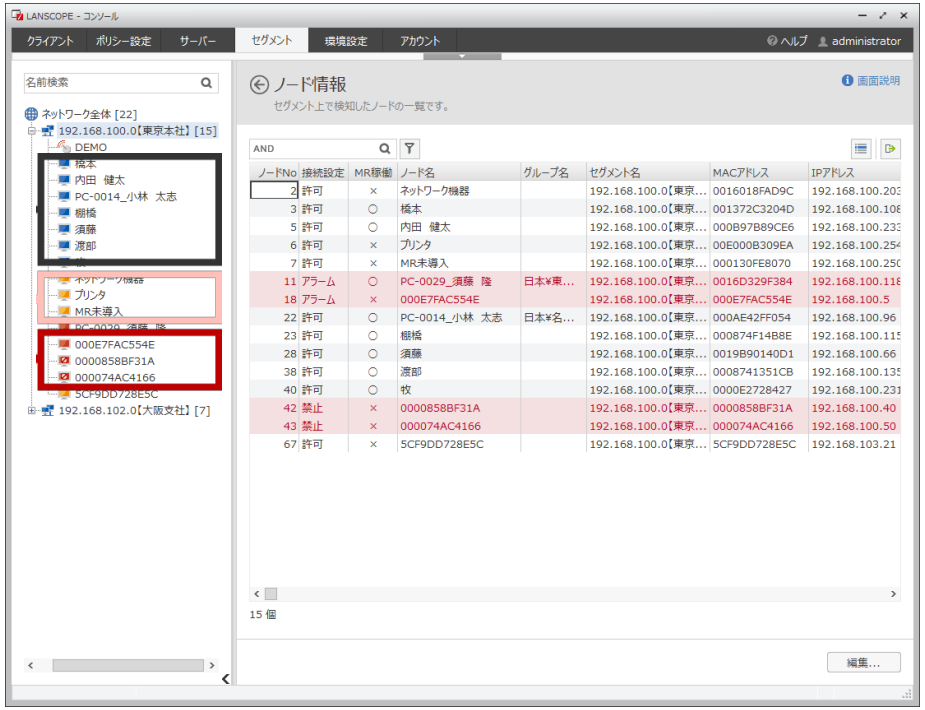
(ア)職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。

不正PC検知・遮断

私物パソコンからの庁内ネットワーク接続を検知・遮断できます

セキュリティ上、ネットワークとの接続には適切な管理が必要であるため、職員の私物パソコンなど、管理者の許可がないパソコンを庁内に持ち込んで有線でネットワークに接続した際は管理者に通知または遮断できます。





LANSCOPE on-premises

6.1　コンピュータ及びネットワークの管理

(6)ログの取得等

①統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

ログ管理

PC操作を記録し、セキュリティモラル向上や問題発生時の詳細調査ができます

パソコンの操作履歴をログ化し収集可能です。情報セキュリティポリシーに反する操作が発生した場合、LANSCOPEが自動で対策すべき問題操作をお知らせします。管理者は問題操作のみ対策を行うだけでOKです。

また、気になる日時・クライアント・部署がある場合、それらをキーに収集したログから細やかに検索・解析を行う事も可能です。

LANSCOPE on-premises

6.1　コンピュータ及びネットワークの管理

(15)電子メールの利用制限

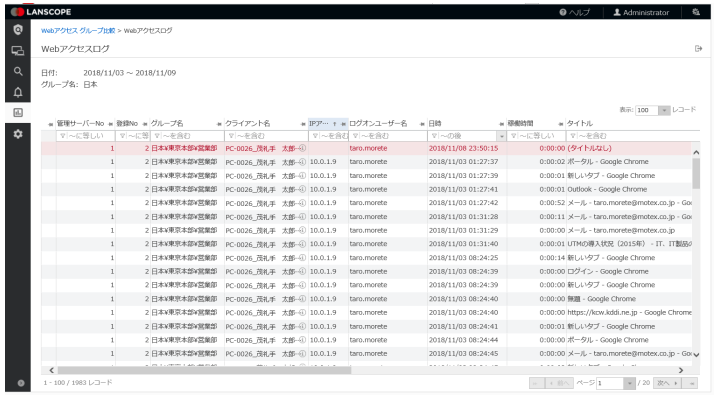
⑤職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない。

Webアクセス管理

クラウドストレージ、Webメール利用ログ取得が可能

クラウドストレージへのアップロード・ダウンロードのログを取得し、情報漏えい経路を監視できます。また、Web メールの送信内容として、送信元、送信先、件名、本文の内容を取得します。アクセス元のURLを指定することで利用を禁止することも可能です。

●クラウドストレージ・Webメール利用ログ



●クライアント型Webフィルタリング

※Mac端末管理非対応

対応サービス

クラウドストレージ
- Dropbox
- Google Apps for Work
- Office365

Web メール
- Gmail
- Outlook.com
- Outlook Web App

Webフィルタリングカテゴリ				
不法	出会い	コミュニケーション	成人嗜好	趣味
主張	金融	ダウンロード	オカルト	宗教
アダルト	ギャンブル	職探し	ライフスタイル	政治活動・政党
セキュリティ・プロキシ	ゲーム	グロテスク	スポーツ	広告
	ショッピング	話題	旅行	未承諾広告

LANSCOPE on-premises

6.1　コンピュータ及びネットワークの管理

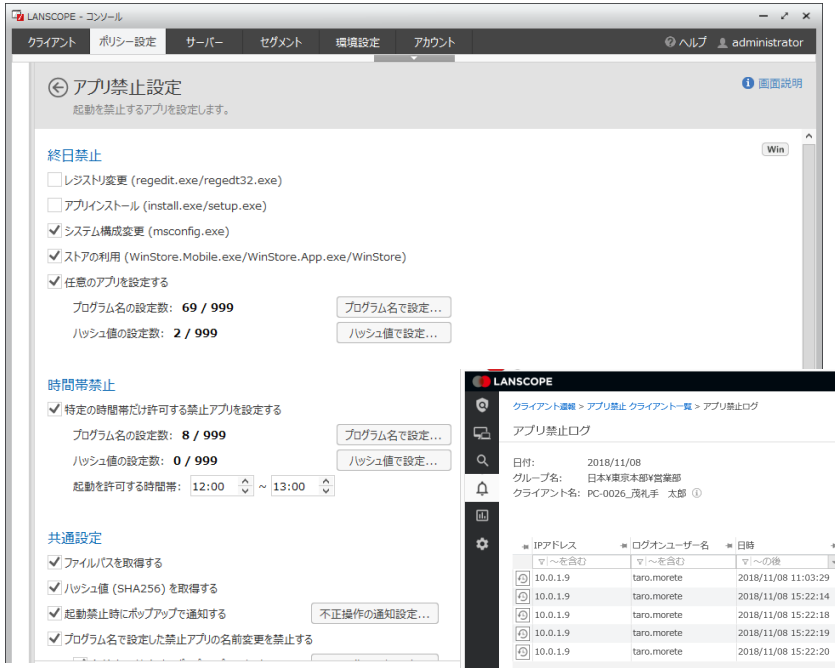
(17)無許可ソフトウェアの導入等の禁止

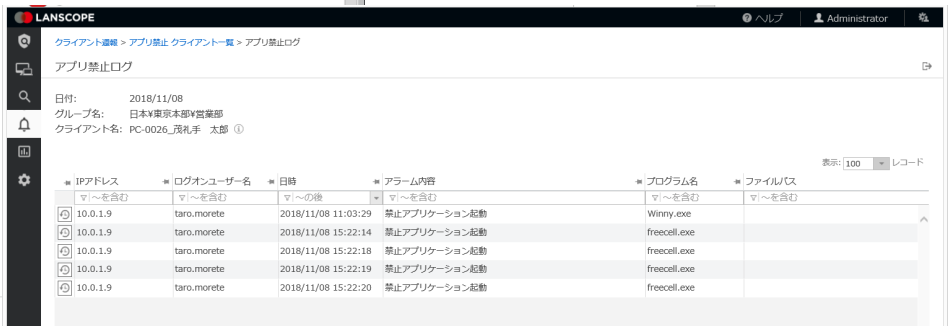
①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

アプリ管理

許可なくパソコンにソフトウェアを インストールできないように禁止できます

インターネットからソフトウェアをダウンロードしてパソコンにインストールすると不正プログラムに感染するといった可能性があります。そのため、職員が勝手にソフトウェアをインストールできないようパソコンを制限する対策が必要です。





LANSCOPE on-premises

6.1　コンピュータ及びネットワークの管理

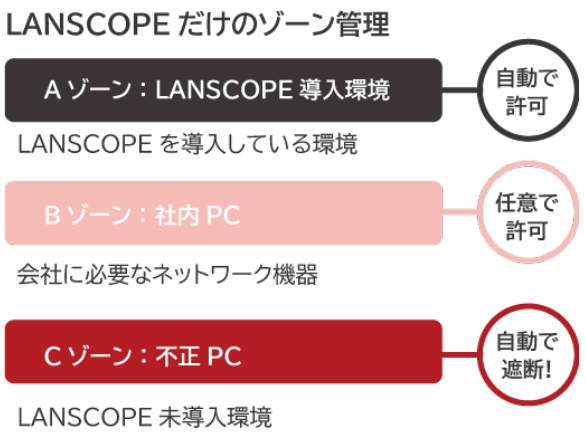
(19)無許可でのネットワーク接続の禁止

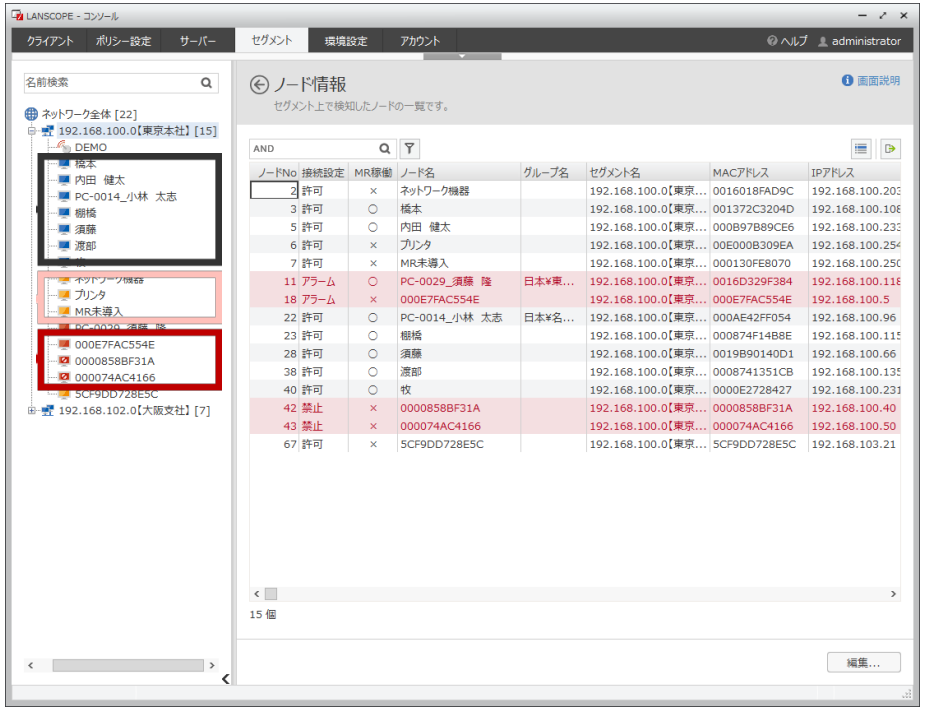
職員等は、統括情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

不正PC検知・遮断

私物パソコンからのネットワーク接続を検知・遮断できます

セキュリティ上、ネットワークとの接続には適切な管理が必要であるため、私物パソコンなど、管理者の許可がないパソコンを庁内に持ち込んで有線でネットワークに接続した際は管理者に通知または遮断できます。





LANSCOPE cloud

6.1　コンピュータ及びネットワークの管理

(20)業務以外の目的でのウェブ閲覧の禁止

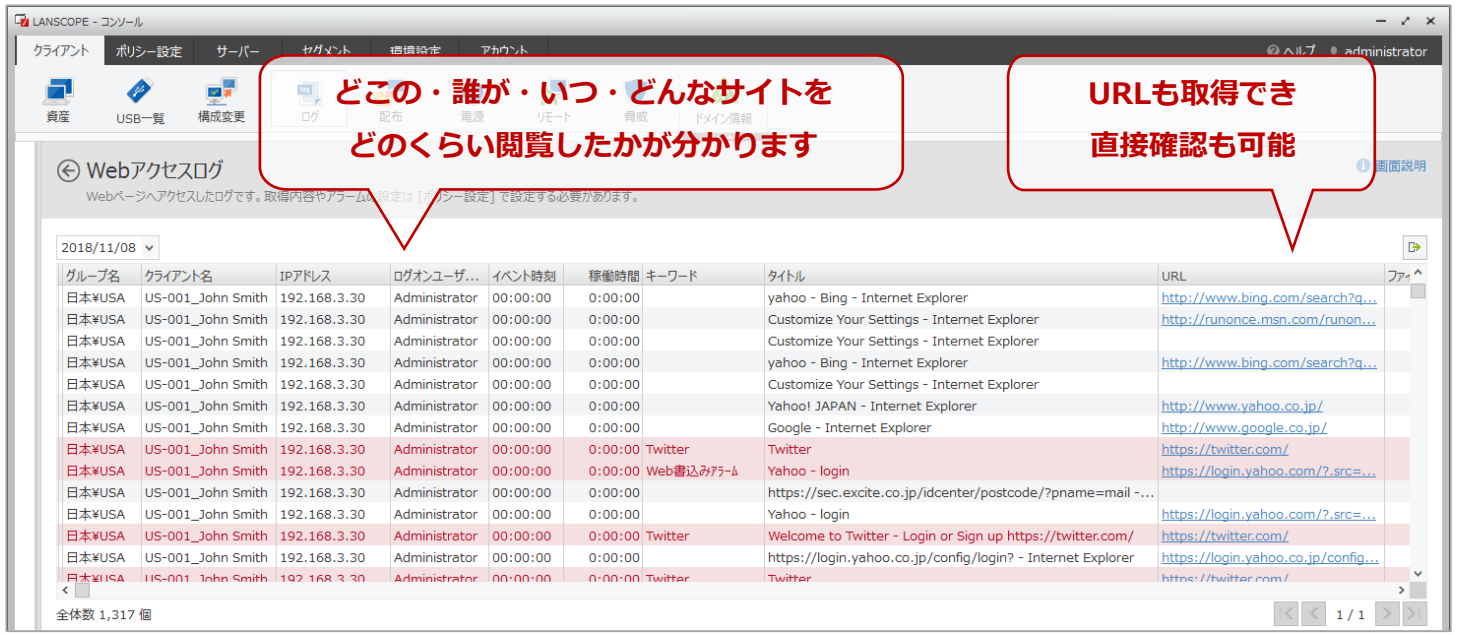
①職員等は、業務以外の目的でウェブを閲覧してはならない。

②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

Webアクセス管理

インターネットアクセス履歴をログ化し収集
カテゴリごとにフィルタリングできます

Webサイトの閲覧記録、特定Web サイトやカテゴリごとの閲覧制御ができます。ユーザーの適切なWeb 利用を促進し、有害サイトへのアクセスを防ぎます。



BlackBerry Protect

6.4　不正プログラム対策

(1)統括情報セキュリティ責任者の措置事項

④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは常に最新の状態に保たなければならない。

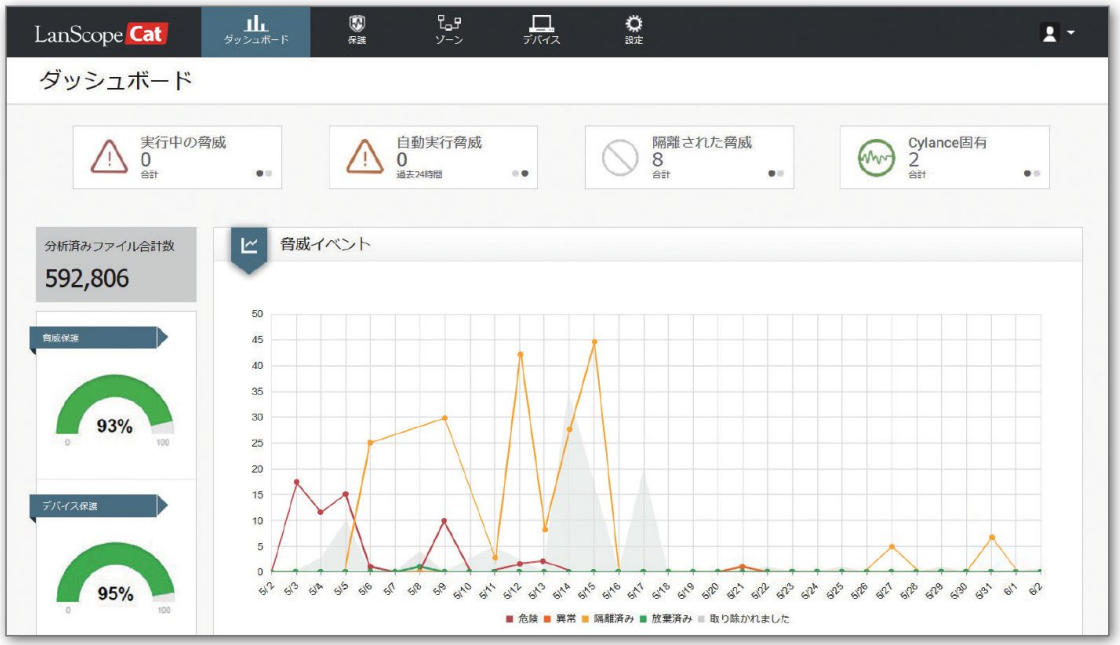
⑥不正プログラム対策のソフトウェアは常に最新の状態に保たなければならない。

マルウェア対策

AI エンジンを活用し、未知のマルウェアも99%以上※の精度で検知・隔離できます

AIエンジンを活用した新技術でマルウェアを検知し、端末をマルウェア感染から保護します。
これまでのウイルス対策ソフトやふるまい検知、サンドボックスのように止められないことが前提の事後対策ではなく、未知の脅威でも実行前に検知し防御することができます。

※　2018 NSS Labs Advanced Endpoint Protection Test 結果より



LANSCOPE on-premises

6.6.セキュリティ情報の収集

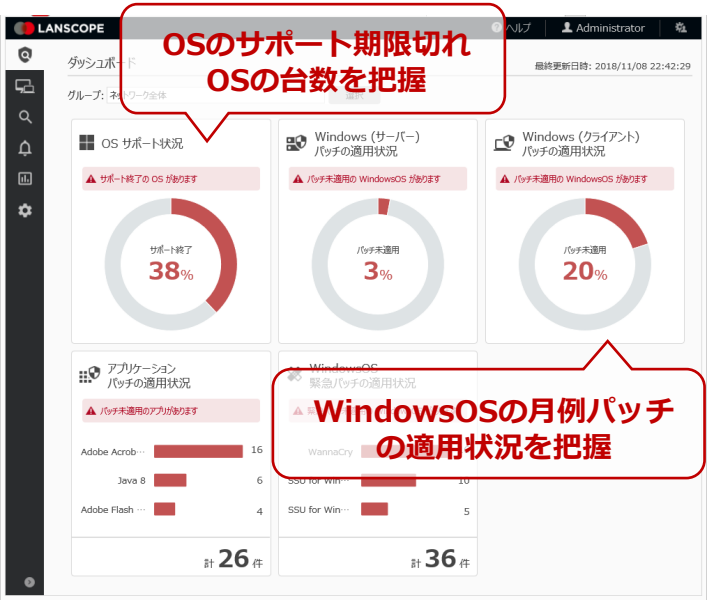
(1)セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

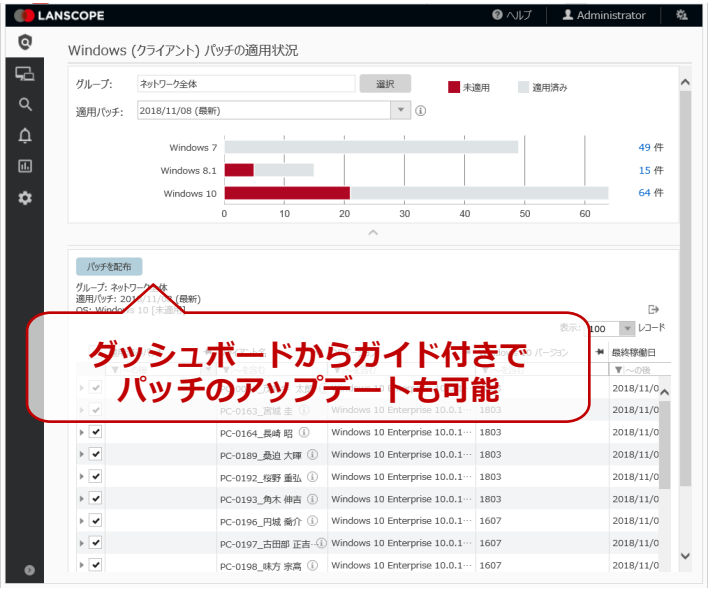
統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

ダッシュボード

脆弱性の有無が一目で分かり その対策が簡単にできます

ダッシュボードでは、組織に存在する端末の中で、最新の状態に保たれていない脆弱な端末を自動で抽出しカードに表示します。カードの詳細には適用すべきパッチの情報を含んでいるため、専門的な知識がなくても、必要な対策を実施できます。対策情報はMOTEX から更新されるので、毎日ダッシュボードを確認するだけで、庁内の脆弱な端末の発見・対策を実現します。





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