LANSCOPE

BlackBerry. Protect

テレワークセキュリティガイドラインに対する対応

本資料は2021年5月版総務省「テレワークセキュリティガイドライン第5版」に基づいて作成しています。

総務省が企業のテレワーク導入における
情報セキュリティ対策に関する検討のガイドラインとしてもらうことを目的に策定

ガイドラインのポイント

- テレワークとは、在宅勤務やサテライトオフィス勤務、モバイル勤務など幅広い勤務形態を想定。クラウドサービスやゼロトラストセキュリティの考え方を示す
- テレワークを実際に行う際の注意点や検討すべき事を集約。テレワーク方式の解説とそのポイントを紹介
- システム・セキュリティ管理者に加えて、経営者やテレワーク勤務者の立場で実施すべきセキュリティ対策や、一定の費用や組織体制が必要になるなど実施難易度が高いセキュリティ対策も示している

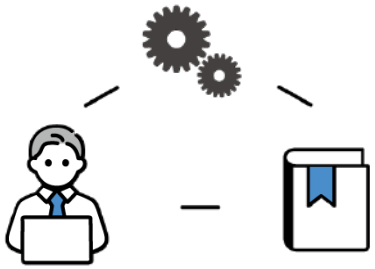
●ガイドラインの想定ターゲット像

役割	経営者システムセキュリティ管理者テレワーク勤務者
セキュリティ予算	外部委託のコストは必要に応じて捻出可能な企業も含めた幅広い組織
セキュリティ推進体制	専任の担当者や担当部門が存在する企業も含めた幅広い組織
セキュリティリテラシ	抽象的な要求事項に対して対応内容の検討や判断を行い対策を実行できるレベル
IT リテラシ	基本的なit用語を理解しているまた基本的なシステムの設定作業が無理なく実施できるレベル

テレワークを実施するために重要な対策・役割を明示化し、最適な環境選択を行います

第５版では、各役割を紹介すると共に、テレワークを取り巻く環境やセキュリティ動向を踏まえ示されています

人・技術・ルールの
バランスの取れた対策

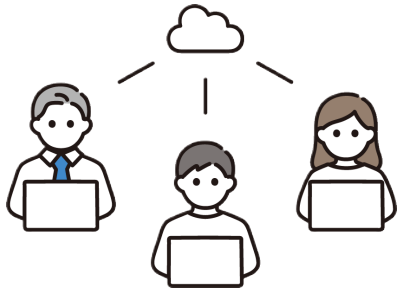


情報資産を守るためには、「ルール」・「人」・「技術」のバランスがとれた対策を実施し、全体のレベルを落とさないようにすることが重要です

経営者・情シス・勤務者
立場に応じた役割分担

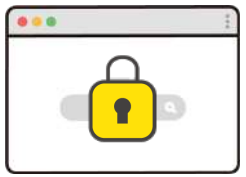
テレワークの実施に当たっては、それぞれの立場からセキュリティの確保に関して必要な役割を認識し、適切に担っていくことが重要です

クラウドサービスの
活用



クラウドサービスは、自組織でサーバ等を自ら保有する必要がありませんが、分類によってはクラウドサービス事業者の提供する資源が変わるため注意が必要です

ゼロトラスト
セキュリティの観点



インターネットと、LANとの境界による防御には限界があり、内部ネットワークにも脅威が存在しうるという考えのもと、セキュリティ強化を行う必要があります

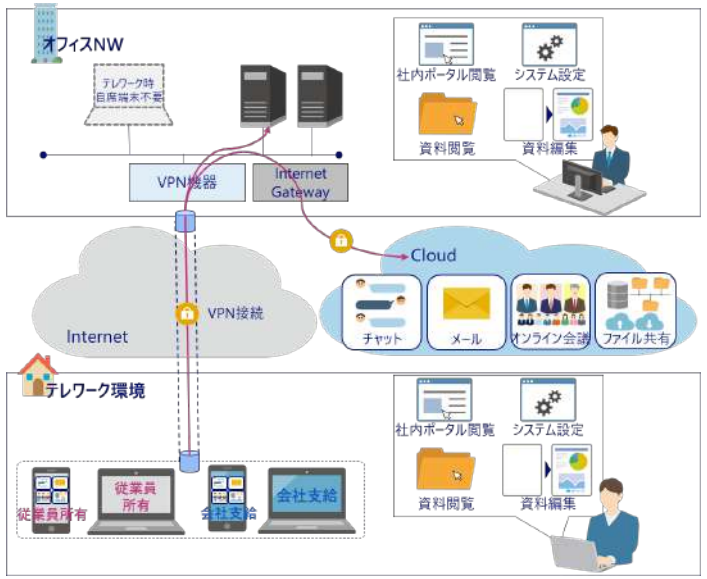
テレワーク方式（システム構成）は大きく７種！メリットデメリットの把握も重要です

方式	概要	メリット	デメリット
① VPN方式	テレワーク端末からオフィスネットワークに対してVPN接続を行い、そのVPNを介してオフィスのサーバ等に接続し業務を行う方法	• オフィス内と同等の業務が可能 • オフィス内と同等のセキュリティレベルの確保が可能 • 通信回線の影響を受けるがテレワーク端末上での作業で回避可	• テレワーク端末のデータ管理とセキュリティ統制が必要
② リモート デスクトップ 方式	テレワーク端末からオフィスに設置された端末（PC等）のデスクトップ環境に接続を行い、そのデスクトップ環境を遠隔操作し業務を行う方法	• オフィスと同等の業務が可能 • オフィス内と同等のセキュリティレベルの確保が可能 • テレワーク端末へのデータ保存制限によりデータ管理が容易	• 通信回線の影響を受けやすい
③ 仮想デスクトップ （VDI）方式	テレワーク端末から仮想デスクトップ基盤上のデスクトップ環境に接続を行い、そのデスクトップ環境を遠隔操作し業務を行う方法	• オフィスと同等の業務が可能 • オフィス内と同等のセキュリティレベルの確保が可能 • テレワーク端末へのデータ保存制限によりデータ管理が容易 • テレワーク端末へのデータ保存制限によりデータ管理が容易	• 通信回線の影響を受けやすい • 大きな環境変更を伴うシステム導入が必要
④ セキュアコンテナ 方式	テレワーク端末にローカル環境とは独立したセキュアコンテナという仮想的な環境を設け、その環境内でアプリケーションを動かし業務を行う方法	• 利用アプリケーション制限によりデータ管理が容易 • テレワーク端末へのデータ保存制限によりデータ管理が容易 • 通信回線の影響を受けるがテレワーク端末上での作業で回避可	• 特定のアプリケーションに業務が限定
⑤ セキュアブラウザ 方式	テレワーク端末からセキュアブラウザと呼ばれる特殊なインターネットブラウザを利用し、オフィスのシステム等にアクセスし業務を行う方法	• 利用アプリケーション制限によりデータ管理が容易 • テレワーク端末へのデータ保存制限によりデータ管理が容易 • 通信回線の影響を受けにくい	• 特定のアプリケーションに業務が限定 • 通信回線の影響を受ける場合がある
⑥ クラウドサービス 方式	オフィスネットワークに接続せず、テレワーク端末からインターネット上のクラウドサービスに直接接続し業務を行う方法	• 必要な数量のみで利用可能 • 比較的軽微な環境変更で利用可能 • オフィスネットワークに接続しないため通信回線の影響なし	• 対応しているクラウドサービスに限定 • テレワーク端末のデータ管理に加えクラウド分散データ管理が必要
⑦ スタンドアロン 方式	オフィスネットワークには接続せず、あらかじめテレワーク端末や外部記録媒体に必要なデータを保存しておき、その保存データを使い業務を行う方法	• システム構築等が不要 • 通信をしない通信回線の影響なし	• 保存されたデータで実施できる業務に限定 • テレワーク端末上のデータ管理とセキュリティ統制が必要

７種類のテレワーク方式（基本構成）

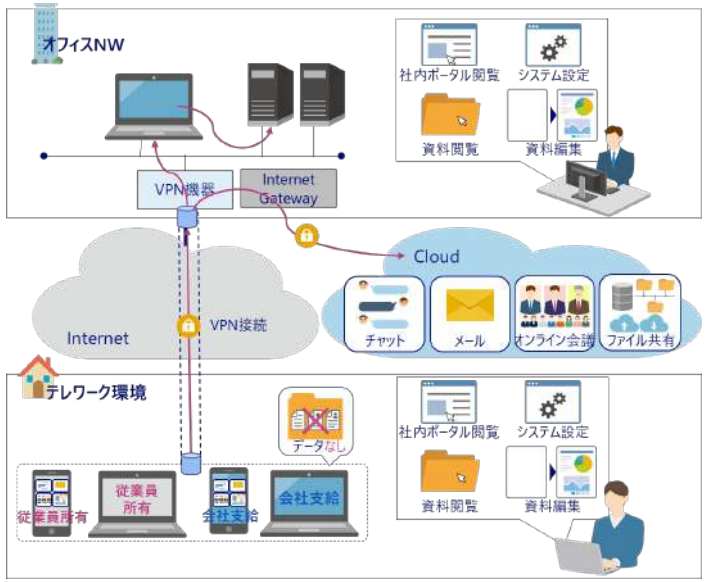
（１）VPN方式

テレワーク端末からオフィスネットワークにVPN接続を行い、オフィスネットワーク内のファイルサーバやクラウドサービス等に接続し業務を行う方法です。テレワーク端末が物理的にオフィス内にある場合と同じように業務が可能です。



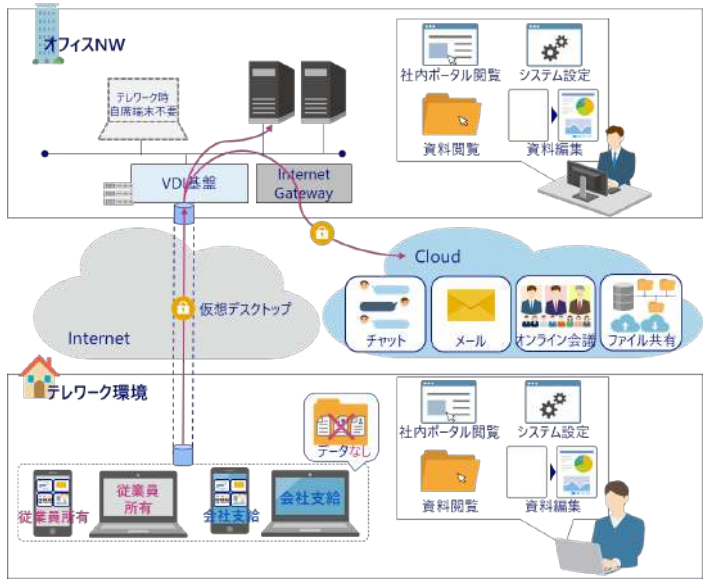
（２）リモートデスクトップ方式

テレワーク端末から、オフィスネットワーク内に設置されたPC等の端末のデスクトップ環境に接続し、当該デスクトップ環境を遠隔操作することで業務を行う方法です。実際にデータ処理を行うのは、遠隔操作されるオフィスネットワーク内に設置されている端末であるため、オフィス内にいる場合と同じように業務が可能です。



（３）仮想デスクトップ（VDI）方式

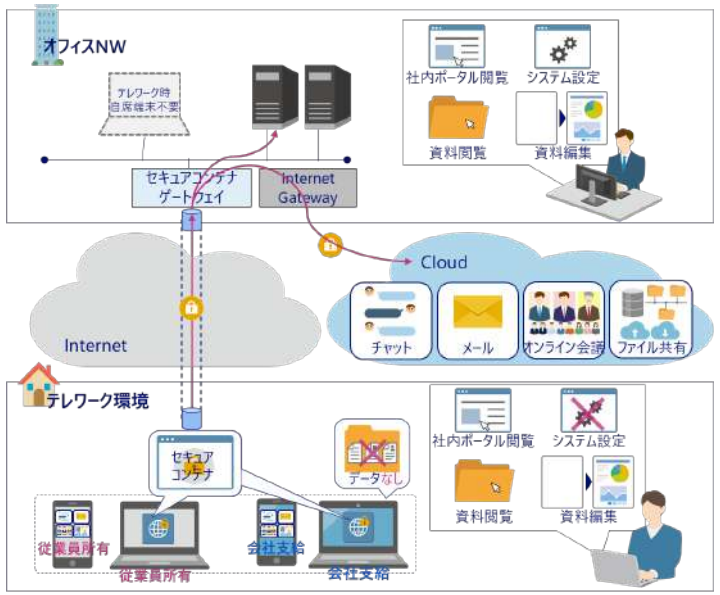
テレワーク端末からオフィスネットワーク内に設置された仮想デスクトップ（VDI）基盤に接続し、当該基盤上のデスクトップ画面を通じて業務を行う方法です。接続するデスクトップ環境を仮想デスクトップ（VDI）基盤（専用サーバ等）に集約させたものです。



７種類のテレワーク方式（基本構成）

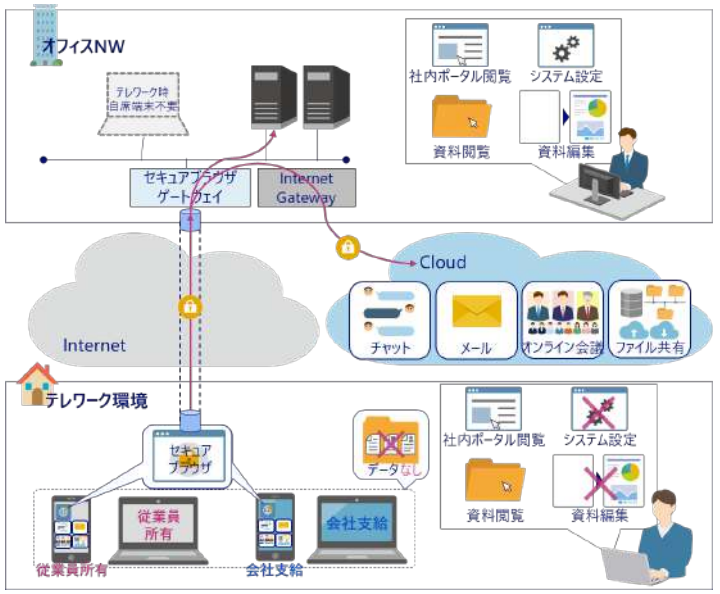
（４）セキュアコンテナ方式

テレワーク端末上に、ローカル環境（テレワーク端末を通常使っている環境）とは独立したセキュアコンテナという仮想的な環境を設け、その仮想環境内でアプリケーションを動作させ業務を行う方法です。



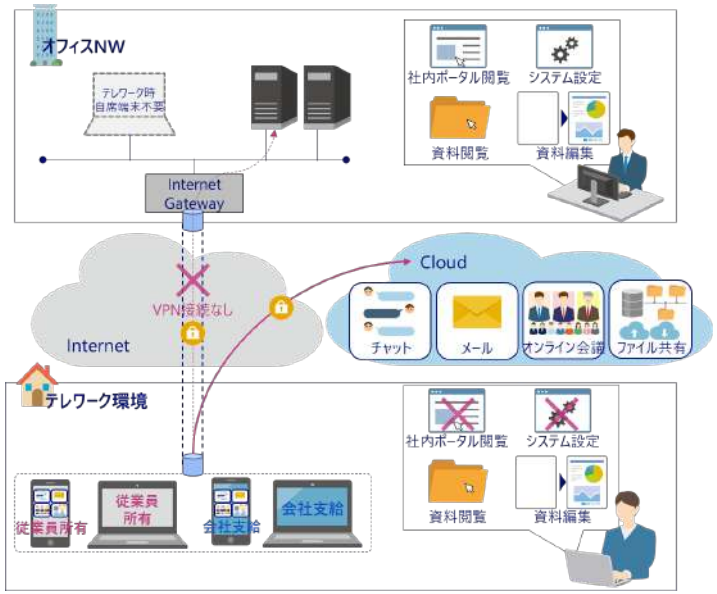
（５）セキュアブラウザ方式

テレワーク端末上で、セキュアブラウザと呼ばれる特別なインターネットブラウザを利用し、オフィスネットワーク内で利用されるシステム（社内システム）やクラウドサービスで提供されるアプリケーションにアクセスし業務を行う方法です。



（６）クラウドサービス方式

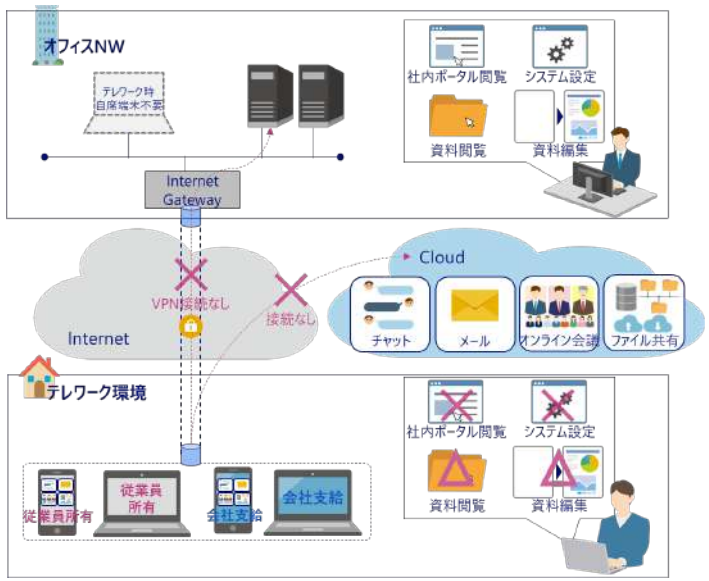
オフィスネットワークに接続せず、テレワーク端末からインターネット上のクラウドサービスに直接接続し業務を行う方法です。テレワーク勤務者はオフィスネットワークを経由せず、クラウドサービスへ直接接続するため、オフィスネットワーク内等にあるテレワークシステムに通信が混雑してしまうといった問題を回避可能です。



７種類のテレワーク方式（基本構成）

（７）スタンドアロン方式

テレワーク時にオフィスネットワークには接続せず、あらかじめテレワーク端末等へ保存していたデータの編集や閲覧をすることで業務を行う方法です。支給端末や個人所有端末をそのまま利用するだけであるため、機器等を新設・増設せずに導入が可能です。またテレワーク利用に伴う通信集中等の問題も生じません。

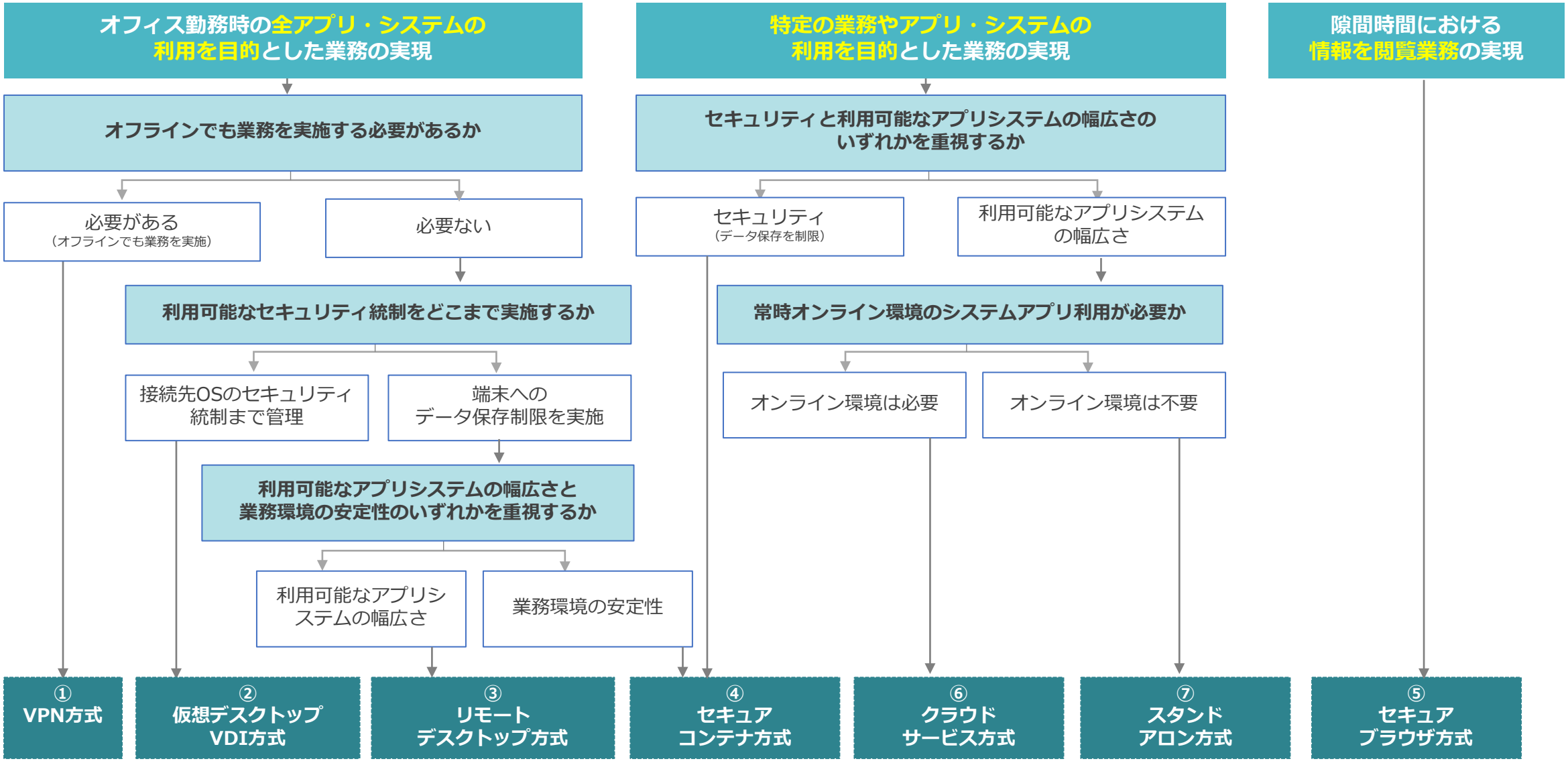


●ガイドライン方式の表記が更新されています

本ガイドライン（第５版）のテレワーク方式	第４ 版で 対応する テ レ ワ ー ク方式
①ＶＰＮ方式	会社PCの持ち帰り方式
②リモートデスクトップ方式	リモートデスクトップ方式
③仮想デスクトップ（VDI）方式	仮想デスクトップ方式
④セキュアコンテナ方式	アプリケーションラッピング方式
⑤セキュアブラウザ方式	セキュアブラウザ方式
⑥クラウドサービス方式	クラウド型アプリ方式
⑦スタンドアロン方式	会社PCの持ち帰り方式

テレワークの方式を選定

自社で「実施しようとする業務」を元に、どの方式が適しているのかを明確にしましょう



業務再現性・通信状況・コスト・導入作業負担・セキュリティ統制の観点でも判断できます

テレワーク方式	オフィス業務の再現性	通信集中時の影響度	システム導入コスト	システム導入作業負荷	セキュリティ統制の容易性	ポイント（想定される使い方）
① VPN方式	S（オフィスと同等の業務が可能）	A（影響を受けるが、端末側(ローカル)作業で一部回避可）	B（システム導入が必要）	B（環境変更を伴うシステム導入が必要）	C（データ管理とセキュリティ統制が必要）	業務再現性が高く、通信集中にも対応したい場合の利用が想定
② リモートデスクトップ方式	S（オフィスと同等の業務が可能）	C（影響を受けやすい）	B（システム導入が必要）	B（環境変更を伴うシステム導入が必要）	A（データ保存を制限でき、データ管理が容易）	業務再現性が高く、セキュリティやコストをバランスする場合の利用が想定
③ 仮想デスクトップ（VDI）方式	S（オフィスと同等の業務が可能）	C（影響を受けやすい）	C（高額なシステム導入が必要）	C（大きな環境変更を伴うシステム導入が必要）	S（データ保存を制限でき、セキュリティの集中管理が容易）	業務再現性が高く、高度なセキュリティを実現したい場合の利用が想定
④ セキュアコンテナ方式	B（特定のアプリケーションやシステムでの作業のみ可能）	A（影響を受けるが、端末側(ローカル)作業で一部回避可）	B（システム導入が必要）	B（環境変更を伴うシステム導入が必要）	A（データ保存を制限でき、データ管理が容易）	セキュリティを確保しつつ通信集中にも対応したい場合の利用が想定
⑤ セキュアブラウザ方式	C（メールや資料閲覧に限定）	B（影響を受けるが影響は軽微）	B（システム導入が必要）	B（環境変更を伴うシステム導入が必要）	A（データ保存を制限でき、データ管理が容易）	セキュリティを重視した、特定業務での利用が想定
⑥ クラウドサービス方式	B（特定のアプリケーションやシステムでの作業のみ可能）	S（オフィスネットワークに接続しないため影響なし）	A（サービス導入費（使用量に応じ必要最小限）が必要）	A（比較的軽微な環境変更で利用可能）	D（データ管理に加え、クラウド上でのデータ管理が必要）	拡張性を重視した、特定業務での利用が想定
⑦ スタンドアロン方式	D（端末に保存したデータのみの作業が可能）	S（通信をしないため影響なし）	S（追加のシステムサービス不要）	S（システム変更不要）	C（データ管理とセキュリティ統制が必要）	コストと導入のしやすさを重視した臨時利用が想定

●特性軸ごとの５段階評価

S：効果や影響が標準よりも相対的に優れている

A：効果や影響が標準よりも相対的にやや優れている

B：効果や影響が標準的である

C：効果や影響が標準よりも相対的にやや劣っている

D：効果や影響が標準よりも相対的に劣っている

評価に当たり、各テレワーク方式は一般的な構成を想定しています。そのため、使用する製品やサービス、具体的なシステム構築方法や構築規模によっては、評価が前後する場合があります。

テレワーク方式にとらわれず、３つの各立場において実施すべき対策が策定されています

（１）
経営者が実施すべき対策

方針・指示

（２）
システム・セキュリティ管理者が実施すべき対策

設定・実施

本資料では
ここに
フォーカス！

（３）
テレワーク勤務者が実施すべき対策

遵守

	対策分類	説明
A	ガバナンス・リスク管理	テレワークの実施に当たってのリスクマネジメントや、情報セキュリティ関連規程（ルール）の整備等に関する対策。
B	資産・構成管理	テレワークで利用するハードウェアやソフトウェア等の資産の特定や、その管理に関する対策。
C	脆弱性管理	ソフトウェアのアップデート実施等による既知の脆弱性の排除に関する対策。
D	特権管理	不正アクセス等に備えたシステム管理者権限の保護に関する対策。
E	データ保護	保護すべき情報（データ）の特定や保存されているデータの機密性・可用性の確保に関する対策。
F	マルウェア対策	マルウェアの感染防止や検出、エンドポイントセキュリティに関する対策。
G	通信の保護・暗号化	通信中におけるデータの機密性や可用性の確保に関する対策。
H	アカウント・認証管理	情報システムにアクセスするためのアカウント管理や認証手法に関する対策。
I	アクセス制御・認可	データやサービスへのアクセスを、必要最小限かつ正当な権限を有する者のみに制限することに関する対策。
J	インシデント対応・ログ管理	セキュリティインシデントへの迅速な対応と、ログの取得や調査に関する対策。
K	物理的セキュリティ	物理的な手段による情報漏えい等からの保護に関する対策。
L	脅威インテリジェンス	脅威動向、攻撃手法、脆弱性等に関する情報の収集に関する対策。
M	教育	テレワーク勤務者のセキュリティへの理解と意識の向上に関する対策。

テレワークセキュリティガイドラインガイドライン対応を行える３つのプロダクト

統合エンドポイント管理

LANSCOPE

LANSCOPE on-premises

IT資産管理・内部不正対策・外部脅威対策をワンストップで対策が可能。様々な環境下でIT管理を統合的に行えるトップシェアプロダクトです

LANSCOPE cloud

PC・スマホ・スマートデバイスを一元管理が可能で、**マルチOSをクラウドにて統合管理**できます。MDM機能に加えPC管理が充実したこれまでにないMDMです

業界最高峰のAIアンチウイルス

CPMS

CPMS Powered by BlackBerry　CPMS Powered by Deep Instinct

AIを活用した高検知のアンチウイルス製品。未知・亜種のマルウェアも99%の高検知が実現。**エムオーテックスオリジナル支援付きで運用も安心**です。

お客様のニーズに応じて、オンプレミス・クラウド版の LANSCOPE をご用意

オンプレミス版

こんな方におすすめ

- サーバーの管理は自社で行いたい
- Azure や AWS など保有している IaaS 基盤で利用したい
- インターネットに接続されないデバイスもまとめて管理したい

クラウド版

こんな方におすすめ

- サーバーの管理やバージョンアップに運用コストをかけたくない
- PC だけでなく、スマホ・タブレットもまとめて管理したい
- 社内 LAN に接続されないテレワークデバイスもリアルタイムに管理したい

（1）経営者が実施すべき対策

ガバナンス・リスク管理	
経営者A - 1 基本対策	テレワーク実施に当たって生じる環境変化を踏まえ、セキュリティポリシー（基本方針）の策定や見直し（システム・セキュリティ管理者にその指示をする。）を行い、見直し後は、テレワーク勤務者にその内容を周知し、方針の共有を行う。
経営者A - 2 基本対策	テレワーク実施に伴うセキュリティ対策の重要性を認識し、セキュリティ対策実施に必要となる組織・人材の組成と予算の確保を行う。
データ保護	
経営者E - 1 基本対策	業務で取り扱う情報について、情報の柔軟かつ有効な活用による事業上のメリットと、情報漏えい等が発生した場合の事業影響等を総合的に勘案し、情報取扱いに関する重要度の方針を定める。
インシデント対応・ログ管理	
経営者J - 1 基本対策	セキュリティインシデント発生時に迅速な対応を可能とするため、事業影響レベルを考慮した対応体制と対応優先度を明確としたインシデント対応計画を策定する（システム・セキュリティ管理者に指示する。）。
教育	
経営者M - 1 基本対策	組織全体でセキュリティへの理解と意識の向上を図るため、セキュリティ研修を実施する（システム・セキュリティ管理者に指示する。）とともに、テレワーク勤務者に対して研修の受講を呼びかける。

（2）システム・セキュリティ管理者が実施すべき対策（LANSCOPEシリーズ対応表）

資産・構成管理		オンプレ	クラウド	CPMS
管理者Ｂ－１ 基本対策	テレワーク端末を管理する台帳を整備する。また、管理対象となるテレワーク端末について、利用状況（シリアルナンバー、OS種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等）を必要に応じて管理・把握する。	○	○	―
管理者Ｂ－２ 発展対策	テレワーク端末の利用状況（シリアルナンバー、OS種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等）について、資産管理ツールを活用し、常に最新の状態を把握できるようにする。	○	○	―
管理者Ｂ－３ 基本対策	テレワーク端末で業務上利用可能なハードウェアやソフトウェア、クラウドサービス等を定め、ルールとしてテレワーク勤務者に周知する。ルール上許可されていないものの利用については、利用者に事前の申請を求め、セキュリティ上の問題がないことを確認できたもののみ利用を許可する。	○	―	―
管理者Ｂ－４ 発展対策	テレワーク端末で利用可能なアプリケーションについて、端末管理ツールを活用し、未許可のアプリケーションのインストールを制限・警告する。	○	○	―
脆弱性管理		**オンプレ**	**クラウド**	**CPMS**
管理者Ｃ－２ 基本対策	オフィスネットワークにアクセスする際に必要となるVPN機器やリモートデスクトップアプリケーション等について、最新のアップデートやパッチ適用を定期的に行う。	○	○	―
データ保護		**オンプレ**	**クラウド**	**CPMS**
管理者Ｅ-４ 基本対策	テレワーク勤務者によるリムーバブルメディア（USBメモリ、CD、DVD等）の使用は、業務上の必要性が認められたものに限定し、ルールで規定する。	○	○	―
管理者Ｅ-８ 発展対策	テレワーク端末にデータを保存することが想定される場合は、内蔵されるHDDやSSDの記録媒体レベルでの暗号化を強制し、テレワーク勤務者で設定を変更できないようにする。また、テレワーク業務で使用するUSBメモリ等も同様に対応する。	○	○	―
管理者Ｅ-９ 基本対策	テレワーク端末の紛失・盗難に備え、MDM（Mobile Device Management）ソリューション等を導入し、有事の際の遠隔制御でのデータ・アカウント初期化、ログイン時のパスワード認証の強制、ハードディスクの暗号化等の機能を有効化する。	○	○	―
管理者Ｅ-10 基本対策	テレワーク端末の紛失時に端末の位置情報を検知するためのアプリケーションやサービス等を導入する。	―	○	―

（2）システム・セキュリティ管理者が実施すべき対策（LANSCOPEシリーズ対応表）

マルウェア対策		オンプレ	クラウド	CPMS
管理者F-1 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。	ー	ー	○
管理者F-2 発展対策	セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能等を用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。	ー	ー	○
管理者F-3 基本対策	テレワーク端末にEDR（EndpointDetectionandResponse）ソリューションを導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。	ー	ー	○
管理者F-4 発展対策	テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。	ー	ー	○
アカウント・認証管理		**オンプレ**	**クラウド**	**CPMS**
管理者H-4 基本対策	テレワーク端末へのログインパスワードや、オフィスネットワークやクラウドサービスにアクセスする際のパスワードは、強力なパスワードポリシーの適用を強制する。	ー	○※1	ー
管理者H-5 基本対策	テレワーク端末やアプリケーションの初期パスワードが強制的に変更されるか、十分な強度のある個別のパスワードが個々に設定されるようにする。	ー	○	ー
管理者H-6 基本対策	利用者認証に一定回数失敗した場合、テレワーク端末の一定時間ロックや、テレワーク端末上のデータ消去を行うよう設定する。	ー	○	ー
アクセス制御・認可		**オンプレ**	**クラウド**	**CPMS**
管理者Ｉ-6 発展対策	オフィスネットワークとインターネットとの通信において、不審なアクセス状況がないか監視する。	○	○	○
インシデント対応・ログ管理		**オンプレ**	**クラウド**	**CPMS**
管理者Ｊ-5 基本対策	不正アクセス等のセキュリティインシデントが発生した際に原因調査が可能となるよう、オフィスネットワーク内に設置されたテレワーク関連機器（VPN装置やVDI機器等）へのアクセスログ、テレワーク関連機器やクラウドサービスにログインした後の認証ログや操作ログ、テレワーク端末の操作ログやイベントログ等）について、ログを取得する。	○	○	ー
管理者Ｊ-6 基本対策	取得したログについて、保存容量を十分に確保する。過去に遡った調査も必要になることがあるため、可能な限り１年以上保存可能とする。	○	○※2	○

※1 iOS/Android デバイスのみ対応　※2 実装予定です。

（2）システム・セキュリティ管理者が実施すべき対策（LANSCOPEシリーズ対応表）

インシデント対応・ログ管理		オンプレ	クラウド	CPMS
管理者Ｊ-９ 発展対策	管理者権限の使用状況や、重要情報へのアクセス履歴については、平時から定期的にログの確認を実施する。	○	○	―
管理者Ｊ-10 発展対策	不審なログが記録された際に、自動的にアラートが通知されるようにする。	○	―	―
教育		**オンプレ**	**クラウド**	**CPMS**
管理者 M-１基本対策	テレワーク勤務者のセキュリティへの理解と意識の向上を図るために、定期的に研修等を実施する。また、テレワーク勤務者に対して最低限求めるセキュリティ対策を定め、テレワーク勤務者に周知する。	セキュリティBOOK		
管理者 M-３基本対策	テレワーク勤務者が自ら実施するセキュリティ対策が適切かどうかを確認する機会を年１回程度設け、その結果を把握する。			

LANSCOPE オンプレミス版・CPMS で行うテレワークセキュリティ対策

一部、オンプレミス版のみで対応できない機能は LANSCOPE クラウド版の内容をご紹介しています。

経営者が実施すべき対策

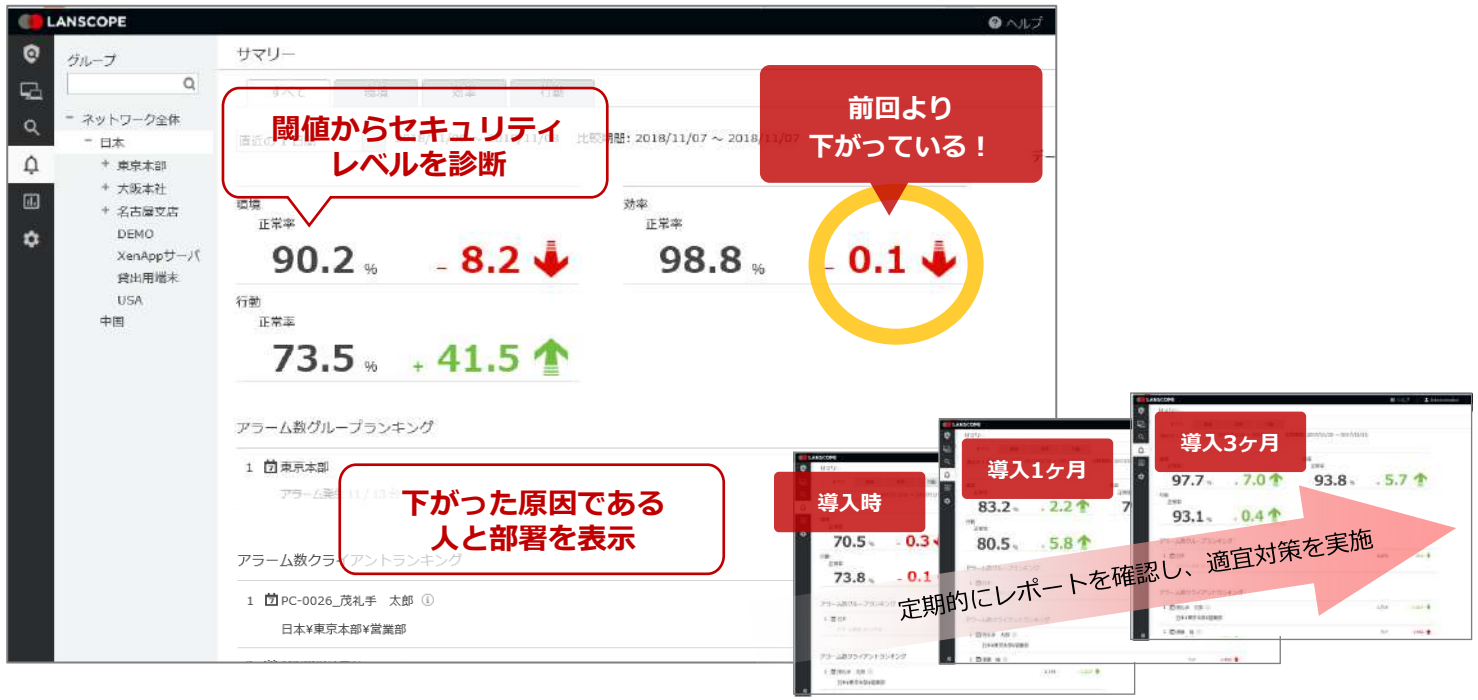
ガバナンス・リスク管理	
経営者Ａ - 1 基本対策	テレワーク実施に当たって生じる環境変化を踏まえ、セキュリティポリシー（基本方針）の策定や見直し（システム・セキュリティ管理者にその指示をする。）を行い、見直し後は、テレワーク勤務者にその内容を周知し、方針の共有を行う。
インシデント対応・ログ管理	
経営者Ｊ - 1 基本対策	セキュリティインシデント発生時に迅速な対応を可能とするため、事業影響レベルを考慮した対応体制と対応優先度を明確としたインシデント対応計画を策定する（システム・セキュリティ管理者に指示する。）。

レポート

従業員の社内ポリシー遵守の傾向を把握できます。

ツールが自動的に組織の問題点を発見・通知するため、検索なしで誰でもポリシーの浸透度を判断できます。

定期的にレポートを確認する事で、経過の観察が可能で、ポリシー尊守のレベルが下がったときも、素早く察知し、改善施策につなげることができます。



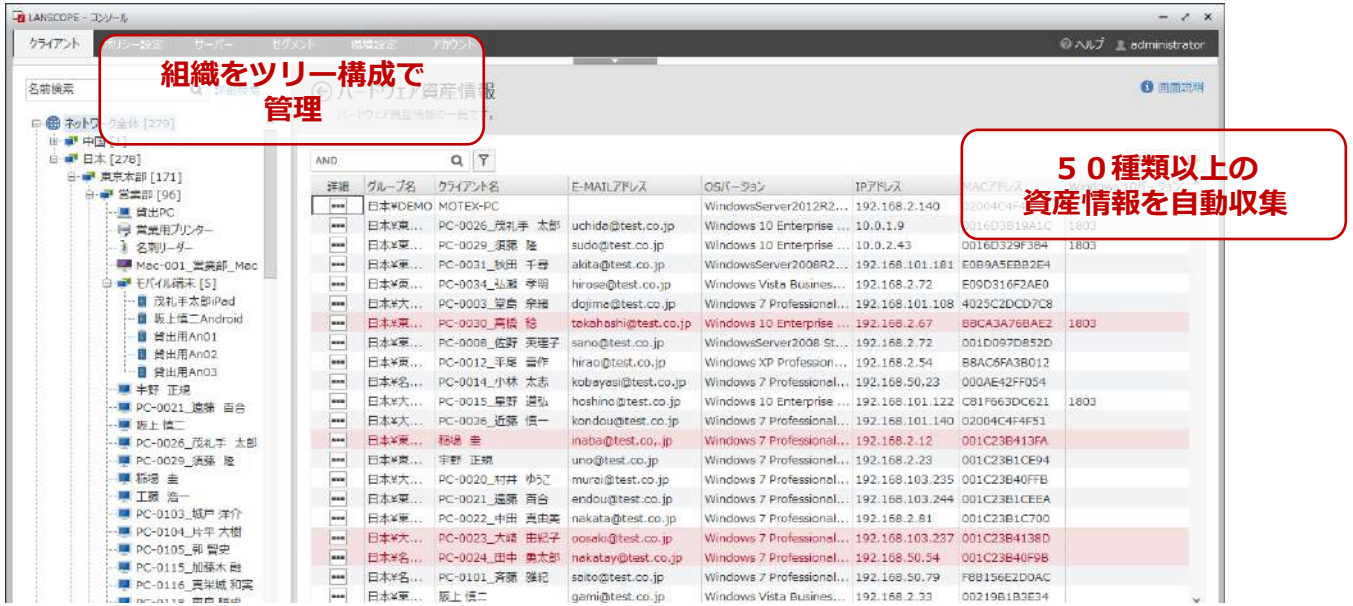
資産・構成管理	
管理者Ｂ - 1 基本対策	テレワーク端末を管理する台帳を整備する。また、管理対象となるテレワーク端末について、利用状況（シリアルナンバー、OS種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等）を必要に応じて管理・把握する。
管理者Ｂ - 2 発展対策	テレワーク端末の利用状況（シリアルナンバー、OS種別・バージョン情報、使用アプリケーション、パッチ適用状況、利用者、所在等）について、資産管理ツールを活用し、常に最新の状態を把握できるようにする。

資産管理機能

ネットワークに接続している機器を把握
最新の資産情報を自動で収集します

ハードウェア／ソフトウェアの情報（IT資産情報）を自動収集し、常に正確な情報を把握できます。

PC以外のプリンターやルーターなどの周辺機器など自動収集できな機器情報もインポートして一括管理ができるのでLANSCOPE上で最新の資産情報の把握が可能です。

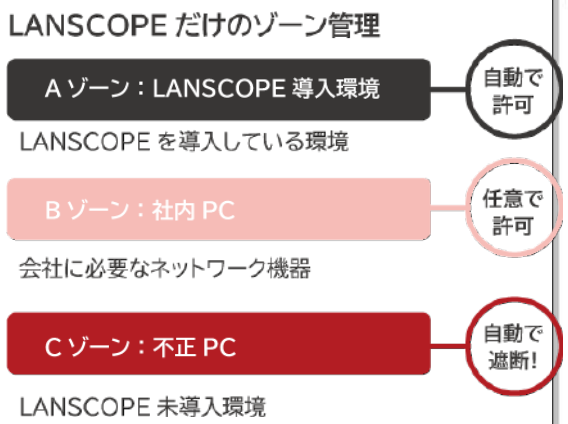


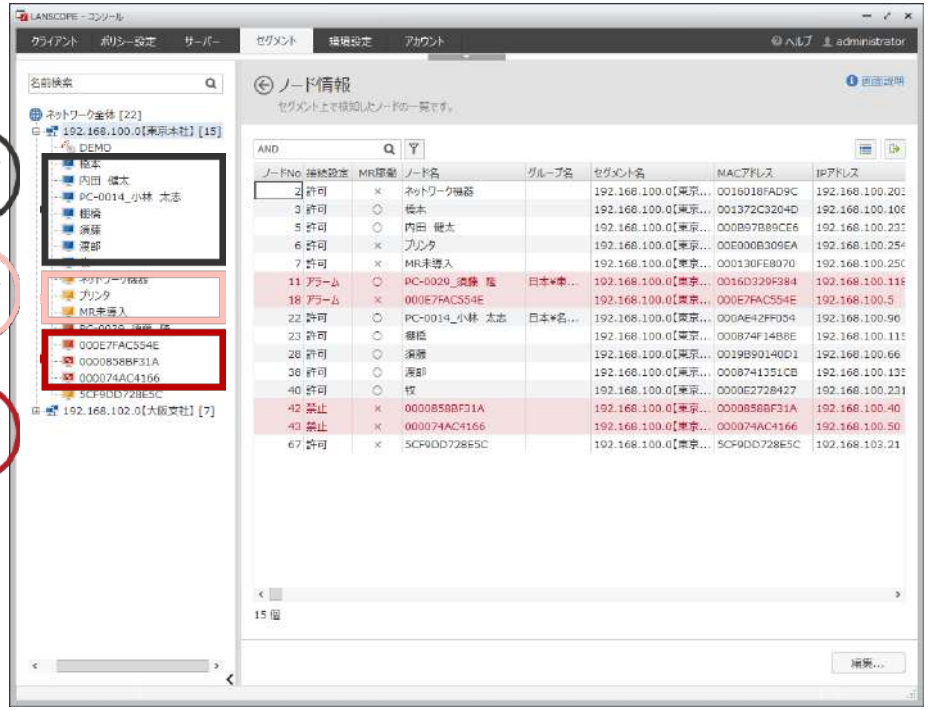
資産・構成管理	
管理者Ｂ - 3 基本対策	テレワーク端末で業務上利用可能なハードウェアやソフトウェア、クラウドサービス等を定め、ルールとしてテレワーク勤務者に周知する。ルール上許可されていないものの利用については、利用者に事前の申請を求め、セキュリティ上の問題がないことを確認できたもののみ利用を許可する。
管理者Ｂ - 4 発展対策	テレワーク端末で利用可能なアプリケーションについて、端末管理ツールを活用し、未許可のアプリケーションのインストールを制限・警告する。

ネットワーク検知機能

ネットワーク上の機器を自動で検知
不正な接続を禁止する事も可能

ネットワークに接続した機器を自動検知／情報収集し、管理対象とすべきIT資産を把握できます。テレワークでは持ち込みPCが発生する可能性が高く、管理者に接続を通知することで不正な接続を制御することが可能です。





■**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を抑えた遮断におススメです

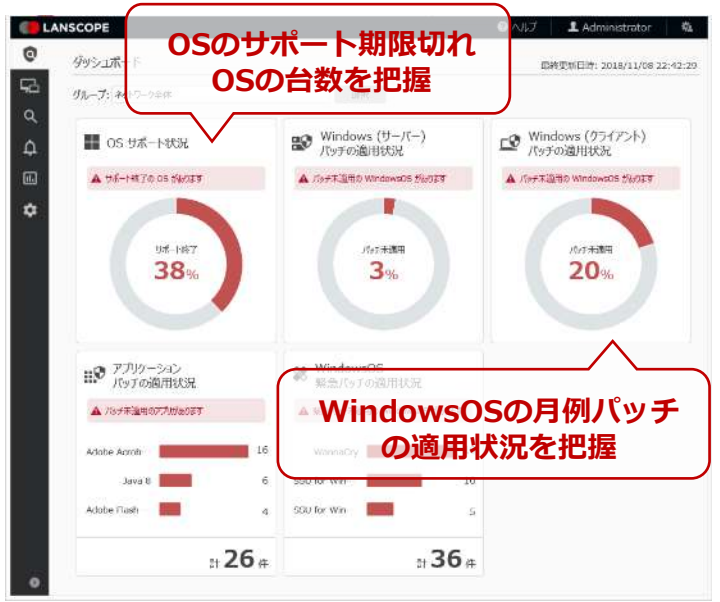
脆弱性管理	
管理者C - 2 基本対策	オフィスネットワークにアクセスする際に必要となるVPN機器やリモートデスクトップアプリケーション等について、最新のアップデートやパッチ適用を定期的に行う。

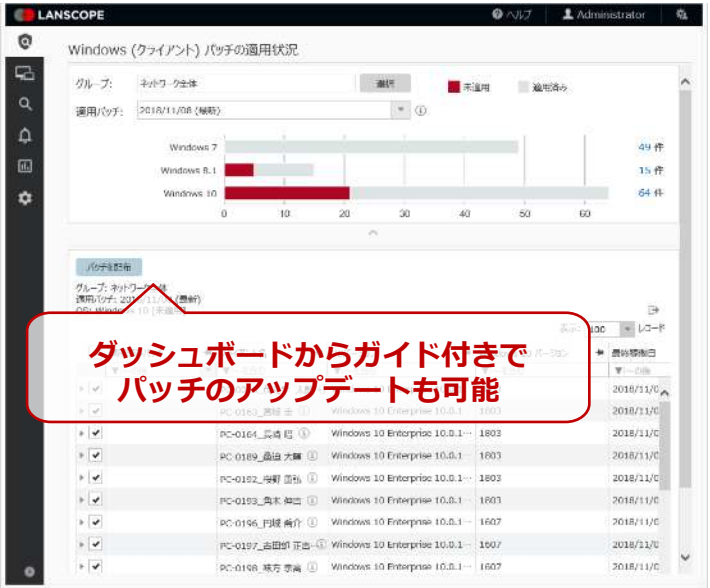
ダッシュボード（脆弱性対策レポート）

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

組織に存在する端末の、OS・セキュリティパッチ・サードパーティー系アプリのパッチ・緊急パッチの適応状況をレポーティングします。

最新でない端末があれば、赤色で表示されるので対策の有無が一目で分かります。常に最新情報を反映しているため、毎日ダッシュボードを確認するだけで、社内の脆弱な端末の発見・対策が可能です。





データ保護	
管理者 E-4 基本対策	テレワーク勤務者によるリムーバブルメディア（USBメモリ、CD、DVD等）の使用は、業務上の必要性が認められたものに限定し、ルールで規定する。

デバイス制御

会社支給以外のデバイスの利用を制御（禁止）できます

社内のデバイスを一元管理し、利用を制御できます。
利便性を活かした「読み取り専用」、特定のデバイスのみ許可する「ホワイトリスト」運用が可能です。
また禁止デバイスが接続されると、ユーザーに禁止通知し、不正利用を抑制が可能です。

■LANSCOPE連携製品　「I-O DATA セキュリティUSBメモリ」

暗号化機能を有するセキュリティUSBメモリで、許可指定USBメモリとして利用できます。

データ保護	
管理者E-9 基本対策	テレワーク端末の紛失・盗難に備え、MDM（MobileDeviceManagement）ソリューション等を導入し、有事の際の遠隔制御でのデータ・アカウント初期化、ログイン時のパスワード認証の強制、ハードディスクの暗号化等の機能を有効化する。
管理者E-10 基本対策	テレワーク端末の紛失時に端末の位置情報を検知するためのアプリケーションやサービス等を導入する。

盗難紛失対策

位置情報・移動履歴の取得が可能で
有事の際にはリモートでロックワイプ

位置情報を取得し、端末がどこにあるのかを可視化することができます。さらに移動履歴も追えるため、盗難紛失時には早急に対応を取る事が可能です。

万が一の場合は、そのまま遠隔でリモートロックワイプが迅速に行えます。

（2）システム・セキュリティ管理者が実施すべき対策

CPMS Cyber Protection Managed Service

データ保護	
管理者 F-1 基本対策	テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
管理者 F-2 基本対策	セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能等を用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
管理者 F-3 発展対策	テレワーク端末にEDR（EndpointDetectionandResponse）ソリューションを導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
管理者 F-4 発展対策	テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。

CPMS（AIアンチウイルス）

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。

CPMS Cyber Protection Managed Service

AIによる予測検知 | **オフラインでも変わらない高い検知率** | **過検知が少ない**

Powered by BlackBerry Protect

- **LANSCOPE連携**をご利用したいお客様
- **インターネット非接続環境**での運用をお考えのお客様
- **レガシーOSへの対応**をお求めのお客様

Powered by deepinstinct BEFORE YOU KNOW IT

- **モバイル対応**をご要望のお客様
- **多くのファイルタイプ**への対応をご要望のお客様
- **EDR要件**への対応をお求めのお客様

アカウント・認証管理	
管理者H-4 基本対策	テレワーク端末へのログインパスワードや、オフィスネットワークやクラウドサービスにアクセスする際のパスワードは、強力なパスワードポリシーの適用を強制する。
管理者H-5 基本対策	テレワーク端末やアプリケーションの初期パスワードが強制的に変更されるか、十分な強度のある個別のパスワードが個々に設定されるようにする。
管理者H-6 基本対策	利用者認証に一定回数失敗した場合、テレワーク端末の一定時間ロックや、テレワーク端末上のデータ消去を行うよう設定する。

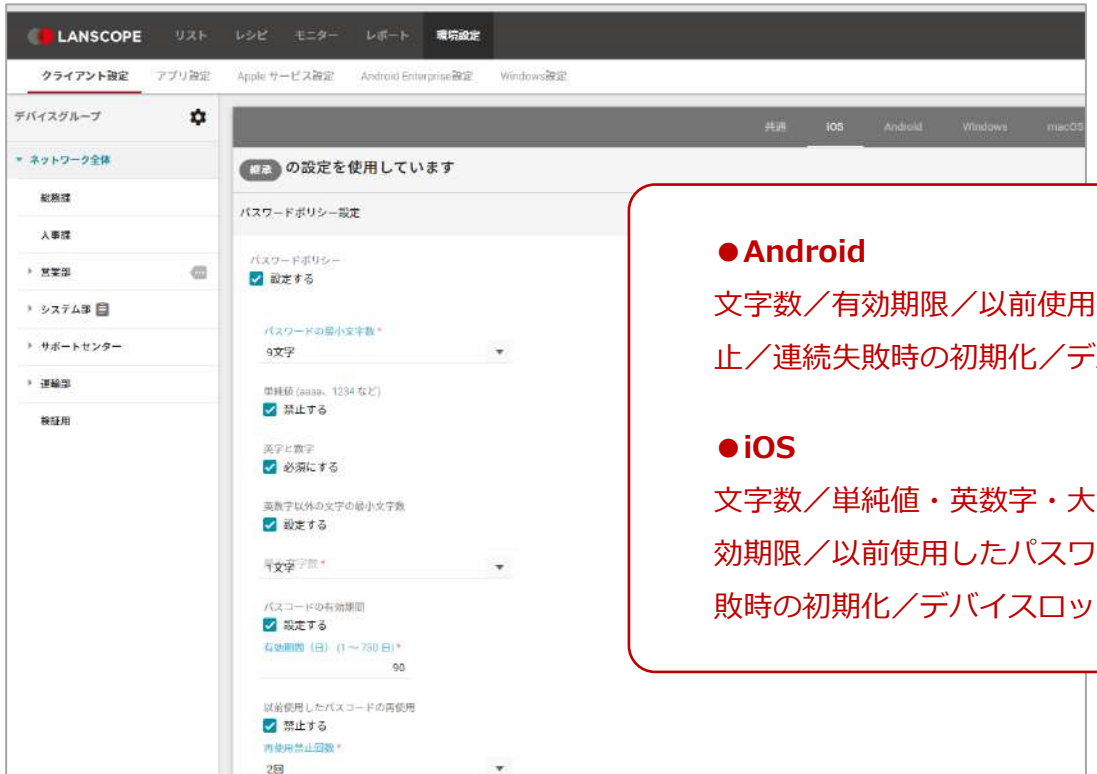
パスワードポリシー

利用端末のパスワードを強化

定期的に変更するなどの働きかけも可能

パスワードの桁数や、英字、数字、複合文字使用など、会社共通のパスワードポリシーをデバイスに一括で適用できます。

Android・iOSで設定項目は設定できるパスコードに差がありますのでご注意ください



●Android

文字数／有効期限／以前使用したパスワードの禁止／連続失敗時の初期化／デバイスロック時間

●iOS

文字数／単純値・英数字・大文字小文字設定／有効期限／以前使用したパスワードの禁止／連続失敗時の初期化／デバイスロック時間

CPMS Cyber Protection Managed Service

データ保護	
管理者Ⅰ-6 発展対策	オフィスネットワークとインターネットとの通信において、不審なアクセス状況がないか監視する。

CPMS（BlackBerry／DeepInstinct）

マルウェア以外の脅威を未然に発見
調査・封じ込め・復旧まで一連の対応が可能

検知したマルウェア以外の「危険なプロセス」や「コマンドの実行」など「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することで、未然に脅威を察知し、対策することが可能です。

＜ＣＰＭＳは予防にフォーカスしたEDR機能を有しています＞

攻撃防御 ❯ 検知 ❯ 調査 ❯ 封じ込め ❯ 復旧

Powered by

BlackBerry Protect

・オプション機能として提供（BlackBerry Optics）
・定期レポートなどサービスが充実

Powered by

deepinstinct BEFORE YOU KNOW IT

・簡易的なEDR機能を標準機能として実装
・事前防御にフォーカス・根本対策のためのEDR機能

LANSCOPE on-premises

インシデント対応・ログ管理	
管理者J-5 基本対策	不正アクセス等のセキュリティインシデントが発生した際に原因調査が可能となるよう、オフィスネットワーク内に設置されたテレワーク関連機器（VPN装置やVDI機器等）へのアクセスログ、テレワーク関連機器やクラウドサービスにログインした後の認証ログや操作ログ、テレワーク端末の操作ログやイベントログ等）について、ログを取得する。

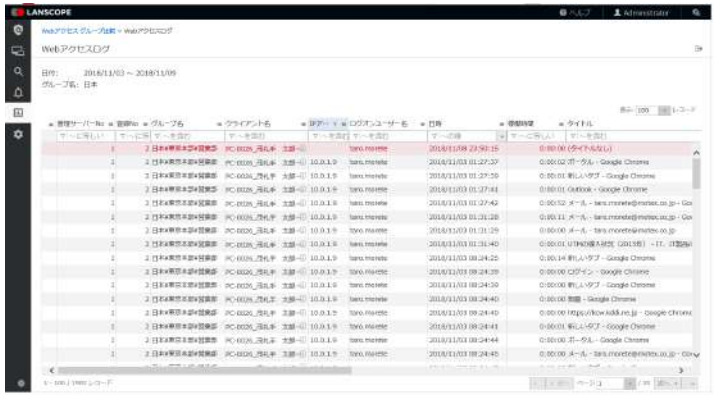
Webアクセス管理

クラウドサービスやWebメールのログを取得
リスクのあるサイトアクセスを制御できます

Webアクセスの閲覧記録、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。

クライアント型のため接続するネットワーク環境などに左右されず、監視や制御ができます。

●クラウドストレージ・Webメール利用ログ



対応Webメール

●Gmail　●Outlook.com　●OutlookWebApp

●クライアント型Webフィルタリング

※Mac端末管理非対応

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

インシデント対応・ログ管理	
管理者Ｊ-６ 基本対策	取得したログについて、保存容量を十分に確保する。過去に遡った調査も必要になることがあるため、可能な限り１年以上保存可能とする。

ログ検索

取得したログを一定期間保存することで検索・調査が可能です

取得した操作履歴（ログ）を様々な条件で検索をかけることが可能です。

よく使う検索条件をあらかじめ保存しておくことで同じ条件でカンタンに検索できます

- **LANSCOPEオンプレミス**
  最大５年保存可能
- **CPMS※**
  最大１年保存可能

※検知エンジンによって異なります

データ保護	
管理者Ｊ-9 発展対策	管理者権限の使用状況や、重要情報へのアクセス履歴については、平時から定期的にログの確認を実施する。
管理者Ｊ-10 発展対策	不審なログが記録された際に、自動的にアラートが通知されるようにする。

PC操作ログ管理

PC操作を記録し、社内ポリシーの遵守の傾向や問題発生時の詳細調査ができます

PCの操作履歴をログ化し収集できます。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、自動で対策すべき問題操作をお知らせするため、管理者は迷うことなく問題操作のみ対策を行えます。

また、ポリシーに抵触する操作が行われた際は、警告のポップアップを出すことで、ポリシーの浸透や意識付けに役立てることも可能です。

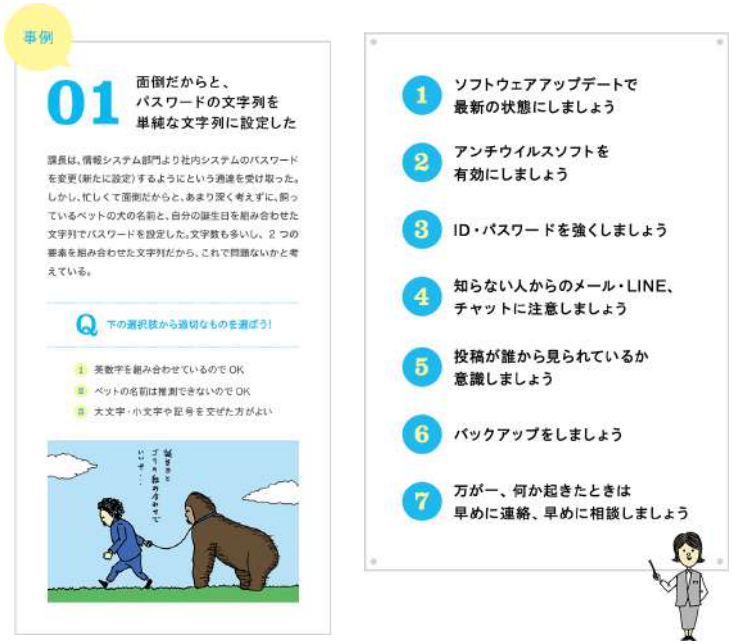
教育	
管理者 M-１基本対策	テレワーク勤務者のセキュリティへの理解と意識の向上を図るために、定期的に研修等を実施する。また、テレワーク勤務者に対して最低限求めるセキュリティ対策を定め、テレワーク勤務者に周知する。
管理者 M-３基本対策	テレワーク勤務者が自ら実施するセキュリティ対策が適切かどうかを確認する機会を年１回程度設け、その結果を把握する。

セキュリティBOOK

情報セキュリティのリテラシー向上のため
分かりやすく、とっつきやすい事例集

どんなに高い投資を行っても、社員一人一人の意識が低いと意味がありません。まず身につけておくべき『セキュリティ習慣』と、身近に起こる様々なリスクをQ&A形式の『20の事例』にまとめました。

セキュリティの基礎を学びたい方や社会人としての教養を身に付けたい方、会社でのセキュリティ研修やマナー研修などにご活用ください。



https://www.motex.co.jp/vision/enlightenment_activity/education_book/

LANSCOPE on-premises

体験版
お試し限定

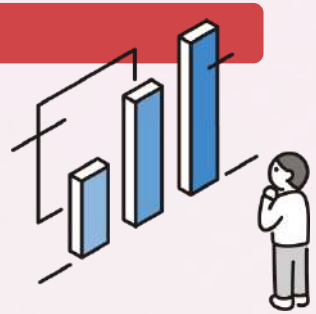
今だけ
レポートサービス
実施中

1ヶ月間 無料体験キャンペーン中

インストールから31日間、LANSCOPE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。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

LANSCOPE cloud

60日間無料体験キャンペーン中

LANSCOPE クラウド版の体験版は 60日間たっぷり利用できます。十分に機能を検証していただき、ご検討ください。設定したポリシーや取得した情報を含め、そのまま製品版へのデータ引き継ぎが可能です。また体験版利用中も、弊社サポートセンターにお電話やメールで問い合わせが可能。体験期間中は、マニュアルやオンラインで学べるトレーニング動画も公開しています

●各種マニュアル・問い合わせが可能

●動画で設定方法を説明

https://go.motex.co.jp/l/320351/2017-06-21/c55z

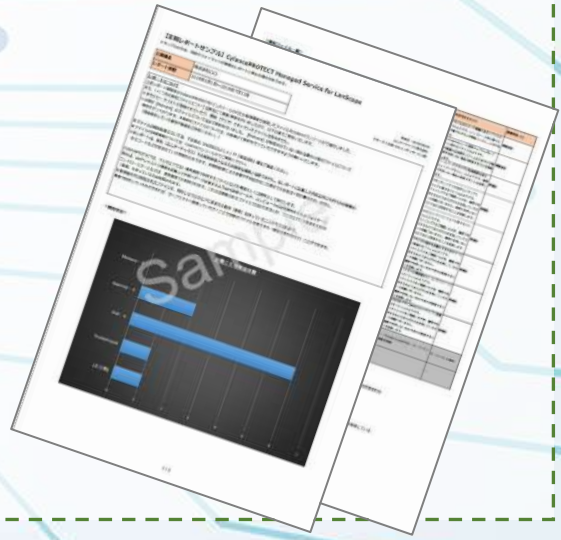
CPMS Powered by BlackBerry

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

※Deep Instinct版アンチウイルス体験は準備中です。ご興味のある方は product@motex.co.jp まで

本資料は2021年5月版総務省「テレワークセキュリティガイドライン第5版」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、対策時には正式版もご参照いただくことを推奨します
総務省：https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

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