



医療業界を狙う凶悪サイバー攻撃に備える！
3省2ガイドラインが示す
今行っておくべき安全管理とは

病院の規模・地域などに関係なく無差別に狙われています！

医療業界をターゲットにしたサイバー攻撃が急増！地域・病院規模関係なく狙われています

徳島県の病院



「ランサムウェア」

徳島県の病院がランサムウェア「LockBit」に感染。約8万5千人分の電子カルテが閲覧できなくなり新規患者の受け入れを停止。最終的に身代金は支払わず、2億円をかけ新システムに刷新。

2021年11月

愛知県の病院



「ブルートフォース攻撃」

愛知県の病院が、パスワードを総当たりで探る「ブルートフォース攻撃」を受け、個人情報を含むメールが流出した。教職員のメールアドレスをかたったスパムメールが送付され発覚した。

2022年3月

インシデントの様々な原因

標的型メール攻撃	主にウイルス（マルウェア）付きのメールを用いて組織や個人を狙う攻撃
ランサムウェア	ファイルを暗号化したり、PCをロックすることで、業務継続を困難にし、復元を条件に「身代金」を要求するマルウェア
ウェブサイトの改ざん	Webサーバに外部から侵入し、Webサイトの内容を書き換えてしまう攻撃
DDoS攻撃	Webサイトやネットワークに過剰なアクセスやデータ送付をすることで、Webサイトへのアクセスができなくなったり、ネットワーク遅延を起こす攻撃
盗難・紛失／メール誤送信	PCやUSBメモリの盗難・紛失や、メールの誤送信等、院内の過失により発生する事故
内部不正	院内の人間や関係者が、個人情報や営業機密を悪意を持って社外に不正に持ち出すなどの行為

医療業界特有の状況・環境に起因。狙われていている今だからこそ一刻も早く対策すべき！！

医療業界のITC化



診療記録などの重要データは機密性が高く、電子カルテ等は命にかかわるものです。そのためランサムウェアによる影響が深刻化しやすく、インシデント発生時は早急に解決を図る可能性が高いと考えられ狙われています。

コロナ禍の多忙さ



新型コロナウイルスの感染拡大で緊急対応を迫られる医療現場は負担が増加、医療ニーズが高まる中に攻撃をすれば、医療機関も身代金の支払う確率が高くなるため狙われやすい傾向にあると考えられます。

システムの脆弱性



コスト削減の観点から、多くの医療機関では古いVPN機器などが使われ続ける傾向にあります。その脆弱性を突くことで攻撃しやすい状態になっている可能性が考えられます。

医療業界のセキュリティ対策は厚生労働省・経産省・総務省の「3省ガイド2ガイドライン」を指標

厚生労働省・経済産業省・総務省が医療業界向けの「3省3ガイドライン」が、対策の効率化を目的に令和2年に「3省2ガイドライン」へ統合



※参考：総務省「医療情報安全管理関連ガイドライン検討ロードマップ」、その他各省庁掲載情報から情報収集し作成

「3省2ガイドライン」は対象によって分けられています。どの対象になるかで使い分けましょう

反面インシデント時の対応など双方のガイドラインに影響した内容も含まれているため、立場に関わらず双方のガイドラインの理解と、場合によっては準拠が必要

	医療情報システムの安全管理に関する ガイドライン	医療情報を取り扱う情報システム・ サービス提供事業者における安全管理ガイドライン
管 轄	厚生労働省	総務省・経済産業省
対 象	患者や介護サービス利用者の個人情報を取り扱う医療機関・薬局・ 介護事業者向け	医療・介護情報システムやサービス提供事業者、医療情報などを預 かる事業者など直接・間接的に関連業務に携わる事業者全てが対象
概 要	個人情報保護法などの法令や電子帳簿法に基づき策定されています。 医療情報の電子化に伴う安全管理について詳細に示しており、具体 的に対策が明記されています。	医療情報の安全管理に関して、医療機関・事業者が担うべき義務・ 責任を策定しています。インシデント発生時の対応方法が示してあ り、各プロセス沿った対策が明記されています。

令和4年3月に最新版5.2版が策定！ 4つの改版ポイントでより理解しやすいガイドラインへ

1	ランサムウェア対策 (6.2章/6.10章)	ランサムウェア攻撃への対応としてバックアップの在り方などを明示。インシデント発生時に速やかに対策を取れるよう、医療情報システムに関する構成図やシステム責任者の義務について明記されている。
2	医療システムと連携する外部サービス・アプリの安全性 (6.5章/6.9章)	安全に管理された環境において、許可したサービスやアプリケーションが利用されているか示すよう追記。BYODの利用において具体的な対策を示すと共に、外部ネットワーク利用時の管理責任が明記されている。
3	電子署名に関する記載の整理 (6.12章)	リモート署名など新形態を受け改版。文書の作成時に資格が必要となる際の署名について要件を明示。その他、長期保存文書に求められるタイムスタンプについてや、暗号アルゴリズムの参照規格をJISからISOの変更などが実施・反映されている。
4	2段階の対応レベルの設定	予てから課題となっていた「分かりづらさ・対策しづらさ」を解決すべく、対策すべき項目を「最低限のガイドライン」と「推奨されるガイドライン」の2項目に分類。医療機関の管理状況や対策基準に合わせて選択・実践できるようになった。

情報セキュリティマネジメントシステム（ISMS）の実践で持続可能なセキュリティ体制の構築をしましょう

ISMSの仕組みに則る事で医療機関ごとにオリジナルで作成する工数が不要に。サイクルを回す事で形骸化しない体制構築を目指す

PLAN

計画

基本方針・運用管理規程などでISMSの構築手順を確立

< 例えば…… >

- 情報セキュリティ方針の決定
- 責任者・担当者選出
- リスクアセスメントなどの手順作成

Planで準備した文書や手順を使って実際にISMSを構築する

DO

実施

< 例えば…… >

- 電子カルテシステムの導入
- USBなどによる持ち出し把握システムの導入
- セキュリティ教育のための勉強会実施

医療機関におけるISMSの実践

< 例えば…… >

- 電子カルテシステムの不要なIDを削除
- 持ち出し可能な暗号化USBを配布
- 問題操作をしたスタッフへ是正

< 例えば…… >

- 電子カルテシステムのアクセスの把握
- 不正な持ち出し状況の有無がないか確認
- インシデントに繋がる人的リスクの把握

処置

ACTION

改善すべき点が出た場合に、是正処置や予防措置を検討。ISMSを維持

Doで構築したISMSが適切に運用されているか監視・見直しをする

点検

CHECK

LANSCOPE に対応する医療ガイドライン

厚労省「医療情報システムの安全管理に関するガイドライン5.2版」対応
6章～10章

6. 医療情報システムの基本的な安全管理

6.5. 技術的安全対策

技術的な対策のみで全ての脅威に対抗できる保証はないため、運用管理による対策との併用は必須である。6.2.3章のリスク分析で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。

- (1) 利用者の識別・認証 (2) 情報の区分管理とアクセス権限の管理 (3) 外部のアプリケーションとの連携における認証・認可
- (4) アクセスの記録（以降、アクセスログという。） (5) 不正ソフトウェア対策 (6) ネットワーク上からの不正アクセス
- (7) 医療等分野における IoT 機器の利用



6.8. 医療情報システムの改造と保守

医療情報システムの可用性を維持するためには、定期的なメンテナンスが必要である。リスク分析で明らかとなった改造と保守において想定される脅威からデータを守るためには、医療機関等の適切な管理の下に保守作業が実施される必要がある。

- ①保守事業者との守秘義務契約の締結、 ②保守要員の登録と管理、 ③作業計画報告の管理、
- ④作業時の医療機関等の関係者による監督等の運用面を中心とする対策が必要である。



6.9. 情報及び情報機器の持ち出し並びに外部利用について

情報又は情報機器の持ち出しについては組織的な対策が必要となり、組織として情報又は情報機器の持ち出しをどのように取り扱うかという方針が必要である。組織的な方針を定めた上で、人的安全対策を施す必要がある。



6.11. 外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理

セキュリティに関して特に留意すべき項目について述べる。医療機関等において外部と個人情報を含む医療情報を交換する場合、医療情報システムを医療機関等が管理する内部ネットワークを通じて外部のネットワークに接続して利用することが考えられる。送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守らなければならない。



6. 医療情報システムの基本的な安全管理

6.5. 技術的安全対策

4. 利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン等の対策を実施させること。
7. アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。
8. アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。
9. アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。
10. システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。
11. 常時不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
12. メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等でやむを得ずファイル送付等を行う場合、送信側で無害化処理が行われていることを確認すること。
15. 無線 LAN を利用する場合、次に掲げる対策を実施すること。
 - (2) 不正アクセス対策を実施すること。少なくとも MAC アドレスによるアクセス制限を実施すること。
16. IoT 機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様である。
 - (3) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法やアップデートが困難な場合に代替措置を講じる方法を検討し、運用すること。

6. 医療情報システムの基本的な安全管理

6.8. 医療情報システムの改造と保守

2. メンテナンスを実施するためにサーバに保守事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。

7. 原則として、保守事業者が個人情報を含むデータを医療機関等外に持ち出させないこと。やむを得ず医療機関等外に持ち出さなければならない場合は、置き忘れ等に対する十分な対策を含む運用管理規程を定めることを求め、医療情報システム安全管理責任者がそれを承認すること。

8. リモートメンテナンスによるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに医療機関等の責任者が確認すること。

6.9. 情報及び情報機器の持ち出し並びに外部利用について

7. 盗難、置き忘れ等に対応する措置として、情報に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。

8. 持ち出した情報機器について、外部のネットワークや他の外部媒体に接続したりする場合は、コンピュータウイルス対策ソフトやパーソナルファイアウォールの導入等により、端末が情報漏洩、改ざん等の対象にならないような対策を実施すること。なお、ネットワークに接続する場合は 6.11 章の規定を遵守すること。

特に、スマートフォンやタブレットのようなモバイル端末では公衆無線 LAN を利用できる場合があるが、公衆無線 LAN は 6.5 章 C.15.の基準を満たさないことがあるため、利用できない。ただし、非常時等でやむを得ず公衆無線 LAN しか利用できない環境である場合に限り、利用を認める。利用する場合は 6.11 章で述べている基準を満たした通信手段を選択すること。

9. 持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除又は停止するか、業務に対して影響がないことを確認すること。

6.11. 外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理

12. クローズドなネットワークで接続する場合でも、内部トラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルや OS のセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。

7. 電子保存の要求事項について

7.3. 保存性の確保について

保存性とは、記録された情報が法令等で定められた期間にわたって真正性を保ち、見読可能にできる状態で保存されることをいう。診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、例えば下記のものと考えられる。

- ・ コンピュータウイルスや不適切なソフトウェア等による情報の破壊及び混同等
- ・ 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取り
- ・ 障害等によるデータ保存時の不整合
- ・ 不適切な保管・取扱いによる情報の滅失、破壊
- ・ 媒体・機器・ソフトウェアの不整合による情報の復元不能

保存性の確保に対するこれらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。

具体的には、不正ソフトウェアによる情報の破壊及び混同等、不適切な保管・取扱いによる情報の滅失、破壊、記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取り、媒体・機器・ソフトウェアの不整合による情報の復元不能、障害等によるデータ保存時の不整合など原因に対する技術面及び運用面での対策が求められる。なおサイバー攻撃等については、6.10章を参照すること。



8. 診療録及び診療諸記録を外部に保存する際の基準

8.3. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準

医療機関等が外部の事業者に対してとの契約に基づいて確保した安全な場所に保存する場合には、データセンター等の情報処理を受託する事業者が総務省・経済産業省の定めた「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の要求事項を満たしていることを確認し、契約等でその遵守状況を明らかにしなくてはならない。外部保存を受託する事業者の選定基準や情報の扱い、情報の提供にあたっては、病院、診療所、医療法人等が適切に管理する場所に保存する場合、又は医療機関等が外部の事業者等との契約に基づいて確保した安全な場所に保存する場合のそれぞれにおいて、適切に対応する必要がある。



8.5. 責任の明確化

ネットワークを通じて外部に保存する場合、医療機関等の管理者の権限や責任の範囲が、自機関等の施設とは異なる施設や電気通信事業者にも及ぶために、より一層、個人情報の保護に配慮することが必要となる。なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存を受託する事業者との契約期間が終了した場合でも、個人情報が存在する限り配慮する必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。ネットワークを通過する際の個人情報保護は、通信手段の種類によって個別に考える必要がある。



7. 電子保存の要求事項について

7.3. 保存性の確保について

【医療機関等に保存する場合】

1. 不正ソフトウェアによる情報の破壊、混同等の防止

(1) 不正ソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体を適切に管理すること。

2. 不適切な保管・取扱いによる情報の滅失、破壊の防止。

(4) 電子的に保存された診療録等の情報に対するアクセス履歴を残すとともに、その履歴を適切に管理すること。

3. 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止

(1) 記録媒体が劣化する前に、当該記録媒体に保存されている情報を新たな記録媒体 又は記録機器に複写すること。記録媒体及び機器ごとに劣化が起こらずに正常に 保存が行える期間を明確にするとともに、使用開始日、使用終了予定日を管理して、月に一回程度の頻度でチェックを行うこと。使用終了予定日が近づいた記録媒体 又は記録機器は、そのデータを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程に定めるとともに、関係者に周知徹底する こと。

8. 診療録及び診療諸記録を外部に保存する際の基準

8.3. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準

(9) 外部保存を受託する事業者を選定する際は、(1)から(8)のほか、少なくとも次に掲げる事項について確認すること。

- | | |
|--|----------------------------------|
| a 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況 | b 医療情報等の安全管理に係る実施体制の整備状況 |
| c 不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況 | |
| d 実績等に基づく個人データ安全管理に関する信用度 | e 財務諸表等に基づく経営の健全性 |
| | f プライバシーマーク認定又は ISMS 認証を取得していること |

8.5. 責任の明確化

ISMS の構築は PDCA モデルによって行われる。JIS Q27001:2006 (※) では PDCA の各ステップを次の様に規定している。

P (Plan) では ISMS 構築の骨格となる文書 (基本方針、運用管理規程等) により、ISMS 構築手順を確立する。

D (Do) では P で準備した文書や手順を使って実際に ISMS を構築する。

C (Check) では構築した ISMS が適切に運用されているか、監視と見直しを行う。

A (Action) では改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する

10. 運用管理について

医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・内容があると考えられるので、ここでは、本書の4章から9章の記載に従い、定めるべき管理項目を記載している。

- 1.に電子保存する・しないに拘らず必要な一般管理事項を、
- 2.に電子保存のための運用管理事項を、
- 3.に外部保存のための運用管理事項を、
- 4.にスキャナ等を利用した電子化、
- 5.に運用管理規程の作成に当たっての手順を記載している。

電子保存を行う医療機関等は1.、2.及び4.の管理事項を、電子保存に加えて外部保存をする医療機関等では、さらに3.の管理事項を合わせて採用する必要がある。運用管理規程等の作成に際しては、以下の文書を参照することが有用である。



10. 運用管理について

(4) 一般管理における運用管理事項

- (d) アクセスログ取得と監査の手順 (e) 時刻同期の方法 (f) 不正ソフトウェア対策 (g) ネットワークからの不正アクセス対策

j IoT 機器の利用に関する事項

- (d) セキュリティ上重要なアップデートの方法

(5) 業務委託（システムの運用・保守・改造）の安全管理措置

- (c) アクセスログの採取と確認

(6) 情報及び情報機器の持ち出しについて

- c 持ち出した情報及び情報機器への安全管理措置
d 盗難、紛失時の対応策

(7) 外部の機関と医療情報を提供・委託・交換する場合

- e 従業者による医療機関等の外部からアクセスする場合の運用管理規程
(a) アクセスに用いる機器の安全管理

(10) 監査

- c アクセスログの監査

2. 電子保存のための運用管理事項

(3) 保存性確保

- (a) 不正ソフトウェアによる情報の破壊及び混同等の防止策 b 不適切な保管・取扱いによる情報の滅失、破壊の防止策

LANSCOPE エンドポイントマネージャー ・ LANSCOPE サイバープロテクションによる対応例

医療情報システムの安全管理に関するガイドライン5.2版の対応 抜粋

スクリーンセーバの展開を実施することでセキュリティ対策を実施

6. 医療情報システムの基本的な安全管理

6.5. 技術的安全対策

4. 利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン等の対策を実施させること。

配布設...	配布設定名	作成方法	設定日時	配布物名	配布ク...	配布状況				一覧
						未完了	完了	失敗	状態	
<input checked="" type="checkbox"/>	2 ウィルス対策ソフトインス...		2012/07/28 08:31	ウィルス対策ソフト	2	1	0	1		
<input type="checkbox"/>	3 adobe Readerインスト...	自動	2012/07/28 09:49	Lhaplus	13	7	6	0		
<input type="checkbox"/>	4 ウィルス対策ソフトインス...	自動	2012/07/28 22:58	ウィルス対策ソフト	14	5	8	1		
<input type="checkbox"/>	5 Win10_16299.334...		2018/09/01 19:10	Win10_16299.334...	3	3	0	0		
<input type="checkbox"/>	6 スクリーンセーバ展開		2018/11/09 10:03	HKEY_USERS¥DEFA...	227	227	0	0		

LANSCOPE エンドポイントマネージャーでは、**配布機能でスクリプトファイルをクライアントPCに配布・実行**することにより、スクリーンセーバーを設定させることが可能です。

いつ・どこで・誰が・何を行ったのか操作履歴（ログ）を取得することで証跡に残すことが可能です

6. 医療情報システムの基本的な安全管理

6.5. 技術的安全対策

7. アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。

WebサイトはURL、ファイル操作はファイルパスを取得できます

関連操作や周辺ログで怪しい動きも察知

イベント日時	発生時刻	イベント	プログラム名	ウィンドウタイトル/ファイル
10.0.1.9	2018/11/08 08:34:00	FloCopy	ファイルコピー先	\\192.168.102.241\F【社外】 医療情報取得2016年度受取...
10.0.1.9	2018/11/08 08:34:00	FloCopy	ファイルコピー先	C:\Users\taro.moroto\Desktop\デスクトップ\2016年度受取取集 取.pdf
10.0.1.9	2018/11/08 09:11:00	FloCopy	ファイルコピー先	\\192.168.102.241\PUBLIC\社外\顧客リスト2.XLS
10.0.1.9	2018/11/08 09:11:00	FloCopy	ファイルコピー先	C:\Users\taro.moroto\Desktop\デスクトップ\顧客リスト2.XLS
10.0.1.9	2018/11/08 09:15:00	FloRun	ファイル名変更前	C:\Users\taro.moroto\Desktop\顧客リスト2.XLS
10.0.1.9	2018/11/08 09:18:00	Attached	メール添付	C:\Users\taro.moroto\Desktop\顧客リスト2.XLS
10.0.1.9	2018/11/08 09:18:00	Attached	メール添付	C:\USERS\TARO\MORETEWDESKTOP\今日着席リスト.xlsx
10.0.1.9	2018/11/08 09:30:26	FloDel	ファイル削除	\\filesv1\public\社外\マイナンバー一覧.xls
10.0.1.9	2018/11/08 09:32:00	FloCopy	ファイルコピー先	\\192.168.102.241\PUBLIC\社外\顧客リスト2.XLS
10.0.1.9	2018/11/08 09:32:00	FloCopy	ファイルコピー先	C:\Users\taro.moroto\Desktop\顧客情報2.XLS
10.0.1.9	2018/11/08 09:33:00	FloRun	ファイル名変更前	C:\Users\taro.moroto\Desktop\顧客情報2.XLS
10.0.1.9	2018/11/08 09:36:00	DriveAdd	追加ドライブ	JT-H580VT (複製:ポータブルデバイス) (PANASONIC JT-H580...
10.0.1.9	2018/11/08 09:39:00	FloCopy	ファイルコピー先	JT-H580VT\内部ストレージ\Pictures\商品案内2.xls
10.0.1.9	2018/11/08 09:43:26	FloMake	ファイル作成	\\filesv1\public\社外\マイナンバー一覧.xls
10.0.1.9	2018/11/08 09:45:26	FloRun	ファイル名変更前	\\filesv1\public\社外\マイナンバー一覧.xls
10.0.1.9	2018/11/08 09:45:26	FloRun	ファイル名変更前	\\filesv1\public\社外\マイナンバー一覧 - コピー.vtc

いつ・どこで・誰が・どのくらい・何をしたのかをログとして取得できます。また様々な条件で検索することも可能で、**最大2年分の操作ログを保存**できます。

機密フォルダの「顧客リスト」を「商品リスト」に名称変更して持ち出した!

LANSCOPE エンドポイントマネージャーログは暗号化済で時刻も世界基準に準拠しており整合性がとれています

6. 医療情報システムの基本的な安全管理

6.5. 技術的安全対策

8. アクセスログへのアクセス制限を行い、アクセスログの不当な削除/改ざん/追加等を防止する対策を実施すること。

9. アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。

LANSCOPE エンドポイントマネージャーのログは、PC・サーバともに暗号化されているため、改ざんが不可能です。

LANSCOPE エンドポイントマネージャーの時刻情報は、世界基準に準拠。UTCの時刻を参照しています

ID	グループ名	クライアント名	IPアドレス	ログID	イベント時刻	プログラム名	ウィンドウタイトル	UTC時刻
1	日本*大...	PC-0171_友澤 尊斗		motex	06:00:00	notepad.exe	MRJ仮想.tst - メモ帳	2018/11/07 21:00:00
1	日本*大...	PC-0171_友澤 尊斗		motex	06:00:58	explorer.exe	Program Manager	2018/11/07 21:00:58
1	日本*大...	PC-0171_友澤 尊斗		motex	06:01:00	Ribbons.scr	不明	2018/11/07 21:01:00
1	日本*東...	PC-0031_秋田 千尋	192.168.2.66	tsaki.akita	07:48:30	cpstrayUI.exe	Check Point Endpoint Security	2018/11/07 22:48:30
1	日本*東...	PC-0031_秋田 千尋	192.168.2.66	tsaki.akita	07:48:37	explorer.exe	スタート	2018/11/07 22:48:37
1	日本*東...	PC-0031_秋田 千尋	192.168.2.66	tsaki.akita	07:49:43	FileCopy	ファイルコピー元	2018/11/07 22:49:43
1	日本*東...	PC-0031_秋田 千尋	192.168.2.66	tsaki.akita	07:49:43	FileCopy	ファイルのコピー先	2018/11/07 22:49:43
1	日本*東...	PC-0031_秋田 千尋	192.168.2.66	tsaki.akita	08:05:26	workspeccs.exe	Amazon WorkSpaces	2018/11/07 23:05:26
1	日本*東...	PC-0031_秋田 千尋	192.168.2.66	tsaki.akita	08:06:38	explorer.exe	スタート	2018/11/07 23:06:38
1	日本*東...	PC-0026_茂礼子 太郎	10.0.1.9	teru.morete	08:06:41	_indextool.exe	_indextool	2018/11/07 23:06:41
1	日本*東...	PC-0026_茂礼子 太郎	10.0.1.9	teru.morete	08:06:43	explorer.exe	Program Manager	2018/11/07 23:06:43
1	日本*東...	PC-0026_茂礼子 太郎	10.0.1.9	teru.morete	08:07:12	chrome.exe	メール - taro.morete@motex.	2018/11/07 23:07:12
1	日本*東...	PC-0026_茂礼子 太郎	10.0.1.9	teru.morete	08:09:02	explorer.exe	Program Manager	2018/11/07 23:09:02
1	日本*東...	PC-0026_茂礼子 太郎	10.0.1.9	teru.morete	08:09:03	EMEDITOR.EXE	第2編 * - EmEditor	2018/11/07 23:09:03
1	日本*東...	PC-0026_茂礼子 太郎	10.0.1.9	teru.morete	08:09:18	explorer.exe	Program Manager	2018/11/07 23:09:18
1	日本*東...	PC-0026_茂礼子 太郎	10.0.1.9	teru.morete	08:09:18	orchis.exe	Orchis Launcher - default	2018/11/07 23:09:18
1	日本*東...	PC-0026_茂礼子 太郎	10.0.1.9	teru.morete	08:09:20	EMEDITOR.EXE	第2編 * - EmEditor	2018/11/07 23:09:20

USBメモリなどの記録メディアの利用を制御し、情報漏洩を防止できます

6. 医療情報システムの基本的な安全管理

6.5. 技術的安全対策

10. システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。

LANSCOPE - コンソール

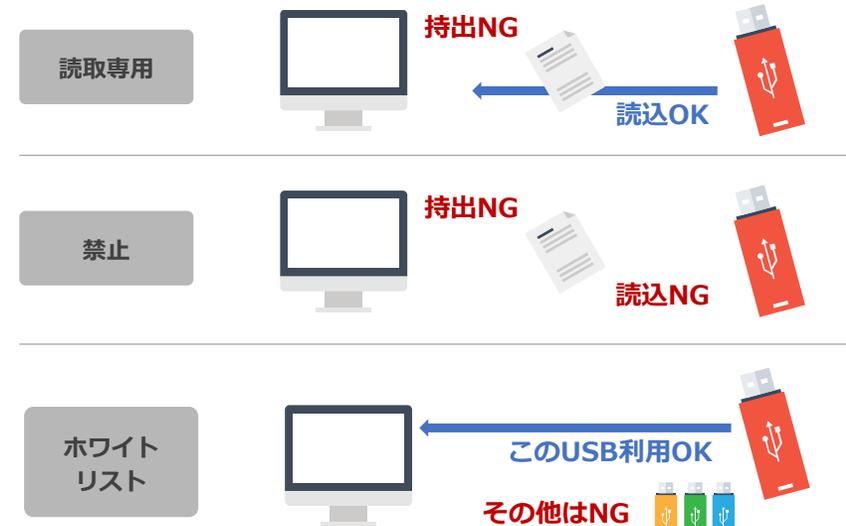
クライアント | ポリシー設定 | サーバー | セグメント | 環境設定 | アカウント

← 端末別の使用制限設定
クライアントごとに設定されているデバイス使用制限の一覧です。

クライアント別にデバイス単位で制御が可能

AND	管...	登録No	グループ名	クライアント名	MRバ...	CD/DVD	FD	USB接続機器	その他の機器
<input type="checkbox"/>	1	1	日本*DEMO	MOTEX-PC	9.3.0.0	読取専用	読取専用	読取専用	読取専用
<input type="checkbox"/>	1	2	日本*東...	PC-0026_茂礼手 太郎	9.0.0.0	読取専用	読取専用	禁止	禁止
<input type="checkbox"/>	1	5	日本*東...	PC-0029_須藤 隆	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	7	日本*東...	PC-0031_秋田 千尋	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	8	日本*東...	PC-0034_弘瀬 孝明	9.0.0.0	読取専用	読取専用	禁止	禁止
<input type="checkbox"/>	1	13	日本*大...	PC-0003_堂島 奈緒	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	15	日本*東...	PC-0030_高橋 稔	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	18	日本*東...	PC-0008_佐野 英理子	9.0.0.0	読取専用	読取専用	禁止	禁止
<input type="checkbox"/>	1	22	日本*東...	PC-0012_平尾 晋作	9.0.0.0	読取専用	読取専用	禁止	禁止
<input type="checkbox"/>	1	24	日本*名...	PC-0014_小林 太志	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	25	日本*大...	PC-0015_星野 道弘	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	29	日本*大...	PC-0036_近藤 慎一	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	30	日本*東...	稲場 圭	9.0.0.0	許可	許可	許可	許可
<input type="checkbox"/>	1	31	日本*東...	宇野 正規	9.0.0.0	読取専用	読取専用	禁止	禁止
<input type="checkbox"/>	1	32	日本*大...	PC-0020_村井 ゆうこ	9.0.0.0	読取専用	読取専用	読取専用	読取専用
<input type="checkbox"/>	1	33	日本*東...	PC-0021_遠藤 百合	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	34	日本*東...	PC-0022_中田 真由美	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	35	日本*大...	PC-0023_大崎 由紀子	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止
<input type="checkbox"/>	1	36	日本*名...	PC-0024_田中 勇太郎	9.0.0.0	禁止 (内蔵/外付け)	禁止 (内蔵/外付け)	禁止	禁止

USBメモリなどのデバイス利用を制御し院内のデバイスを一元管理できます。また禁止環境下でPC毎やデバイス毎に個別許可するなど、現場に即した運用が可能です



AIを活用した高精度なアンチウイルスで防ぐことが難しいとされる未知のウイルスから守ります

6. 医療情報システムの基本的な安全管理

6.5. 技術的安全対策

10. システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。
11. 常時不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
12. メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等をやむを得ずファイル送付等を行う場合、送信側で無害化処理が行われていることを確認すること。



AIを活用した高精度のサイバーセキュリティソリューションを2つ
の選べる検知エンジンをご用意しています。未知・亜種のマルウェア・ランサムウェアの**検知率は99%**と高検知です！



DNAレベルの
マルウェア解析



AI（人工知能）
による自動判断



毎日のアップ
デート不要

LANSCOPE サイバープロテクション powered by CylancePROTECTが 選ばれるポイント

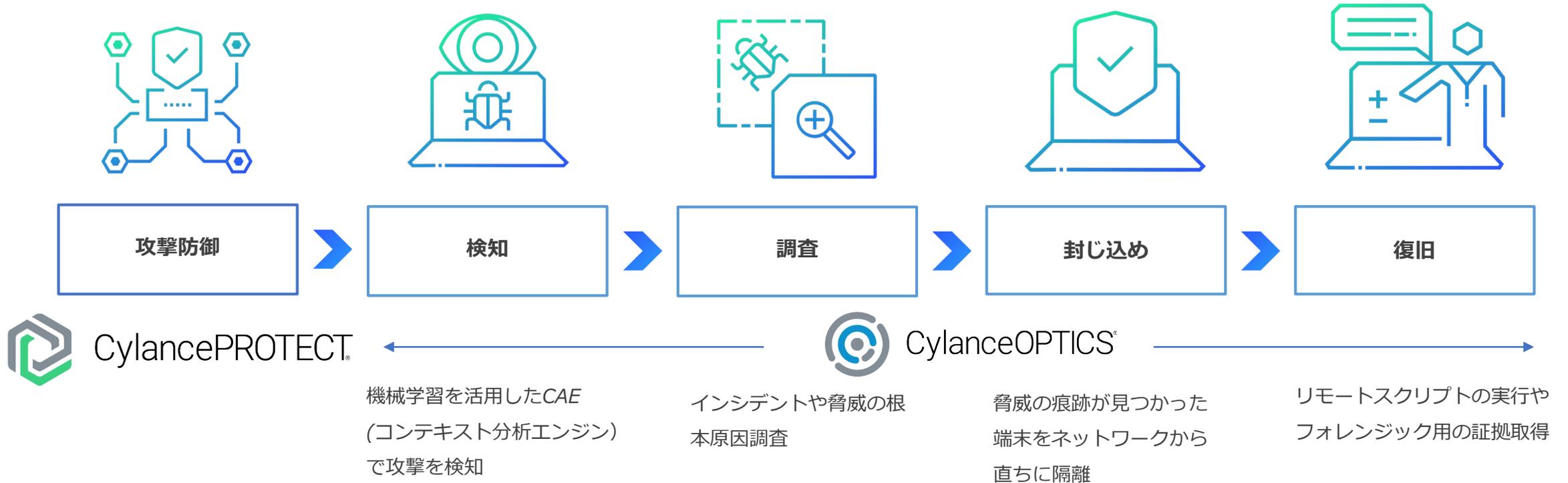
- 未知・既知問わずマルウェアを止められること
- 予測検知という方式で、感染前に止めることが可能
- テレワークなど、あらゆる環境にも対応可能
- PC に掛ける負荷が軽く、動作を妨げず、運用も簡単であること

<実際に予測検知で事前に検知がを支援>

ウイルス名	検知したエンジン	ウイルス名	検知したエンジン
MyWebSearch	26か月前	PolyRansom	28か月前
Emotet	27か月前	GandCrab	26か月前
installCore	27か月前	GoldenEye	13か月前
Petya-Like	20か月前	WannaCry	19か月前

高検知に加え、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EDR機能も利用可能です

本格的に分析したい方にLANSCOPE サイバープロテクションPowered by CylancePROTECTのEDR機能「CylanceOPTICS」がおすすめです



CylancePROTECTと統合

AIを活用

予防にフォーカス

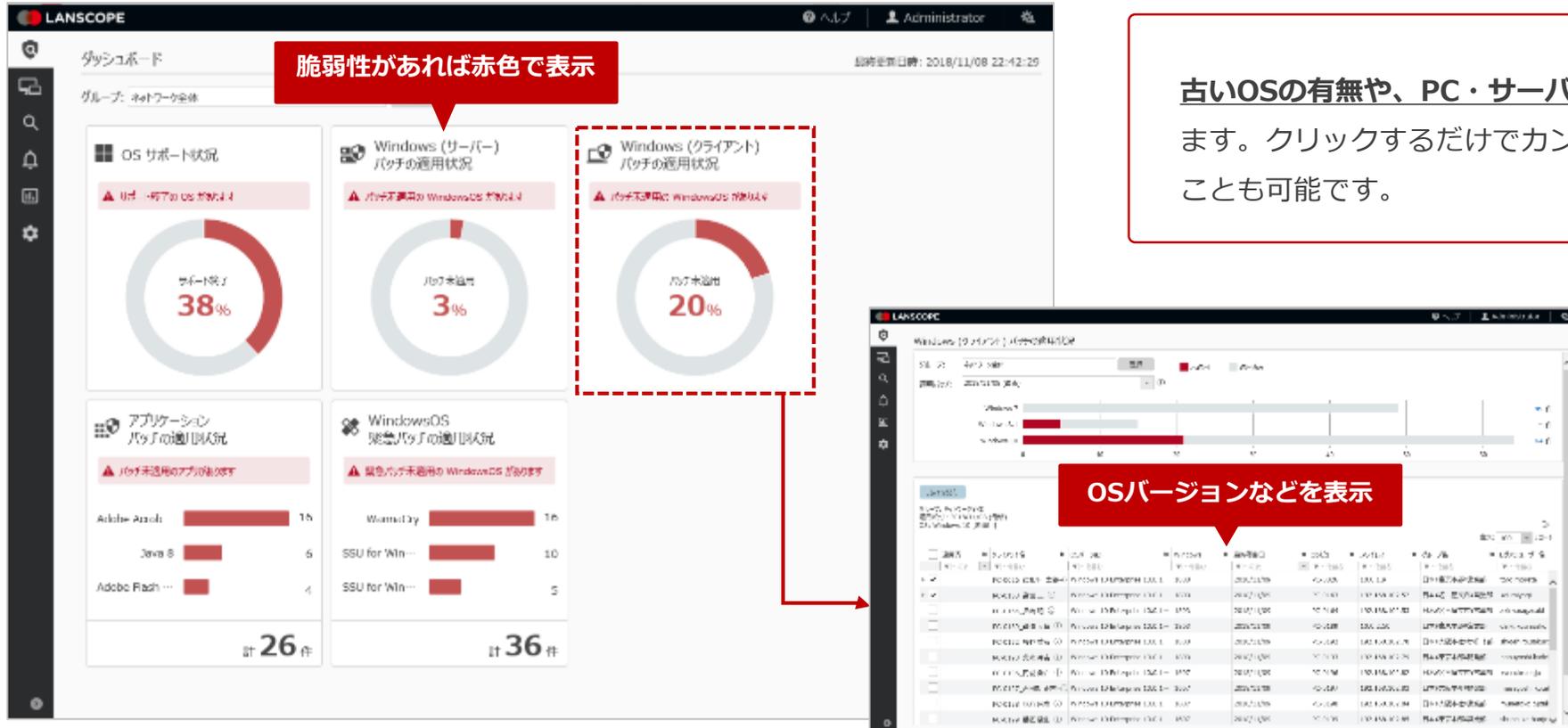
機能更新・品質更新プログラムの適用状況をレポート形式で把握！1Clickで最新のプログラムを適用

6. 医療情報システムの基本的な安全管理

6.5. 技術的安全対策

16. IoT 機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様である。

(3) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法やアップデートが困難な場合に代替措置を講じる方法を検討し、運用すること。



最新の脆弱性情報（JVN注意喚起情報）を表示！ 社内の関連する脆弱性の有無と状況を把握できます

自社内にインストールされているアプリケーションの脆弱性の有無を把握、危険度を把握できます

JVNが注意喚起している情報TOP5を自動表示

JVN脆弱性情報ページの確認ができます

JVNDB番号	タイトル	CVE	発行日	更新日	ベンダー名	対象製品名	スコア (CVSSv3)	攻撃元 (CVSSv3)	攻撃元 (CVSSv2)	対象バージョン	攻撃元区分	参考情報
JVNDDB-001001	Memphis, San Mateo, Project に影響を受けるウェブサイトの脆弱なプラグインに関する脆弱性	CVE-2021-46134	2021-08-18	2021-08-18	Jetty	jetty-embedded	8.8	Critical	7.5	9.0	リモート	https://jvndb.jvn.jp/db/entries/2021-08-18-001
JVNDDB-001002	WordPress における脆弱なプラグインの脆弱性に関する脆弱性	CVE-2021-31320	2021-08-18	2021-08-18	WordPress	WordPress	8.8	Critical	7.5	9.0	リモート	https://jvndb.jvn.jp/db/entries/2021-08-18-002
JVNDDB-001003	WordPress における脆弱なプラグインの脆弱性に関する脆弱性	CVE-2021-31320	2021-08-18	2021-08-18	WordPress	WordPress	8.8	Critical	7.5	9.0	リモート	https://jvndb.jvn.jp/db/entries/2021-08-18-003
JVNDDB-001004	Cloud Application Services Engine における脆弱なプラグインの脆弱性に関する脆弱性	CVE-2021-31320	2021-08-18	2021-08-18	Cloud Application Services Engine	Cloud Application Services Engine	8.8	Critical	7.5	9.0	リモート	https://jvndb.jvn.jp/db/entries/2021-08-18-004
JVNDDB-001005	Linux KVM Hosts Gate Operator における脆弱なプラグインの脆弱性に関する脆弱性	CVE-2021-31320	2021-08-18	2021-08-18	Linux KVM Hosts Gate Operator	Linux KVM Hosts Gate Operator	8.8	Critical	7.5	9.0	リモート	https://jvndb.jvn.jp/db/entries/2021-08-18-005
JVNDDB-001006	Microsoft Windows Server における脆弱なプラグインの脆弱性に関する脆弱性	CVE-2021-31320	2021-08-18	2021-08-18	Microsoft Windows Server	Microsoft Windows Server	8.8	Critical	7.5	9.0	リモート	https://jvndb.jvn.jp/db/entries/2021-08-18-006

① JVN注意喚起情報最新TOP5

日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供するJVNの最新情報を自動収集・表示します。

② 任意の条件でソート、フィルタ可能検索

JVN脆弱性情報やバージョンなど様々な条件でソート・検索することが可能です。

JNVDB番号 / タイトル / CVE / 発行日指定 / 更新日指定
ベンダー名 / 対象製品名 / 危険度 (CVSSv3・CVSSv2) / 攻撃区分

③ 検索結果詳細

②でソート・フィルタした情報を表示します。

- ・ JVN 番号
- ・ タイトル
- ・ CVE
- ・ 発行日
- ・ 更新日
- ・ ベンダー名
- ・ 対象製品名
- ・ 危険度 (CVSS v2,v3)
- ・ スコア (CVSS v2,v3)
- ・ 対象バージョン
- ・ 攻撃元区分
- ・ 参考情報 (URL クリックで JVN 元サイトへリンク)

LANSCOPE エンドポイントマネージャーは現状把握から効果測定が可能のため、PDCAサイクル化に役立ちます

8. 診療録及び診療諸記録を外部に保存する際の基準

8.5. 責任の明確化

ISMS の構築は PDCA モデルによって行われる。JIS Q27001:2006 (※) では PDCA の各ステップを次の様に規定している。

P (Plan) では ISMS 構築の骨格となる文書 (基本方針、運用管理規程等) により、ISMS 構築手順を確立する。

D (Do) では P で準備した文書や手順を使って実際に ISMS を構築する。

C (Check) では構築した ISMS が適切に運用されているか、監視と見直しを行う。

A (Action) では改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する

PLAN

計画

基本方針・運用管理規程などでISMSの構築手順を確立

(1) ドクターの学会等で情報持ち出しの際はUSBメモリの利用申請をして情報持ち出しを行う

(4) USBメモリは支給された暗号化付のUSBメモリの利用に変更

(3) 申請外の利用が散見されたためヒアリングしたところ手間がかかる事が発覚。暗号付きUSBメモリの貸出制に変更

処置

ACTION

改善すべき点が出た場合に、是正処置や予防措置を検討。ISMSを維持

Planで準備した文書や手順を使って実際にISMSを構築する

DO

実施

(2) USBメモリの利用状況を把握するためにエンドポイントマネージャーを導入

(3) エンドポイントマネージャーでUSBメモリの利用状況を把握し申請書と持ち出したデータや頻度などを突合

点検

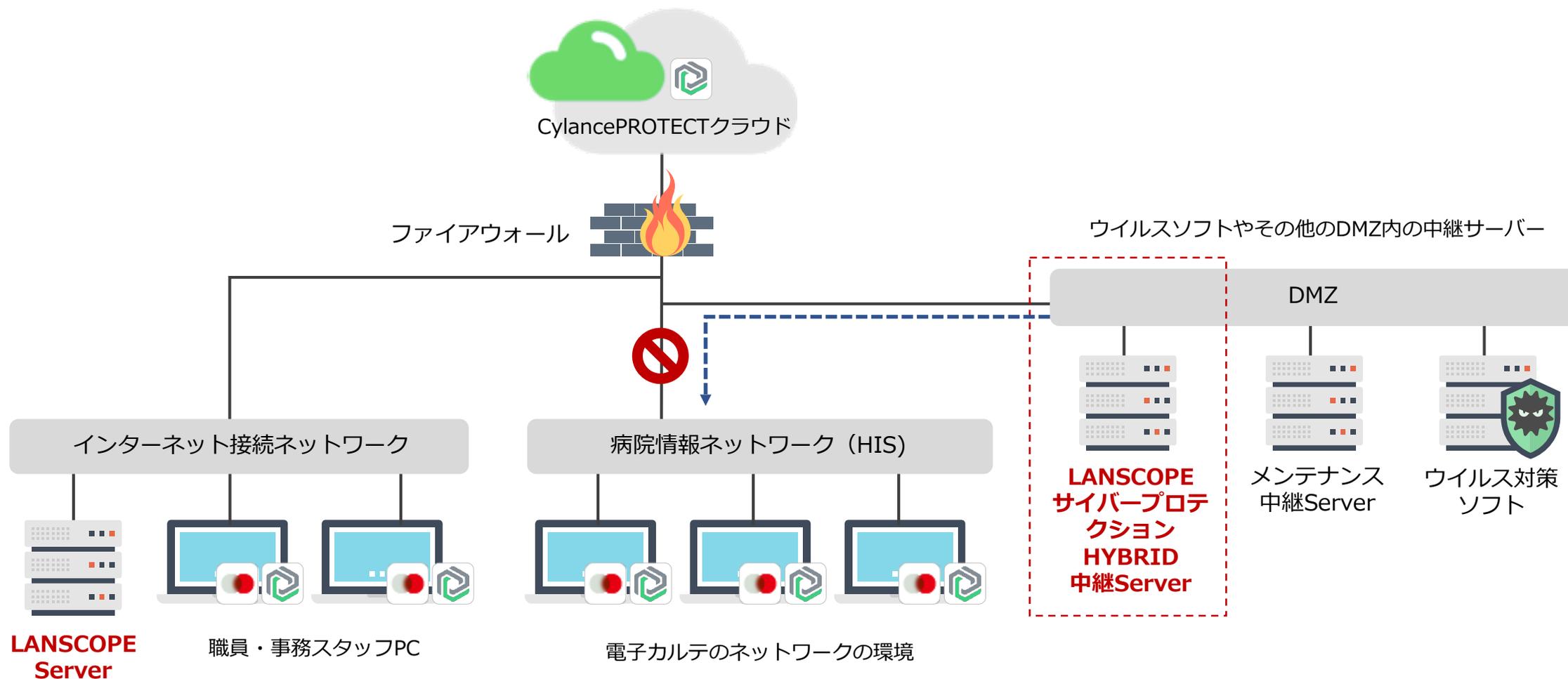
CHECK

Doで構築したISMSが適切に運用されているか監視・見直しをする

医療機関におけるISMSの実践

電子カルテネットワークをセキュアに保つための構成にも対応可能です

医療現場特有のネットワーク構成でも管理が可能！環境に合わせて柔軟に対応できます



※DMZとHISを採用した構成の一例です。環境に合わせて組み合わせは異なりますので詳細はお問い合わせください

【例】 LANSCOPE エンドポイントマネージャー オンプレミス版 × LANSCOPE サイバープロテクション Powered by CylancePROTECT (HYBRID)

ガイドラインに示されているセキュリティ要件をエンドポイントで満たすことが可能です

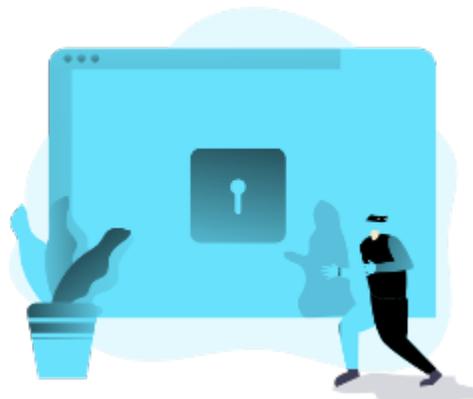
LANSCOPE エンドポイントマネージャーは医療ネットワークにおける情報漏洩をさせない「体制構築」と「万が一の対応」が可能です

情報漏洩対策



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・対策することでリスクある行動を把握、情報漏洩をさせないための体制づくりを支援します。院内に人間はもちろん協力会社の人間の行動も把握できます。

外部脅威対策



常に最新のバージョンを保っているかどうか、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。また検知が難しいとされる未知・亜種のマルウェアにも高精度で対応できます。

万が一の対策



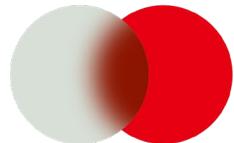
機密情報の入ったPC・スマホの盗難・紛失時も位置情報を取得し検索を行ったり、リモートでロック・ワイプをかけることで情報漏洩を防ぐことが可能です。また暗号化機能Bitlockerの適用状況の把握や、複合キーの一元管理で復旧も効率的に行えます。

LANSCOPE のご紹介

エンドポイント管理ツール「LANSCOPE エンドポイントマネージャー オンプレミス版」

AIアンチウイルス「LANSCOPE サイバープロテクション powered by CylancePROTECT」

IT資産管理・情報漏洩対策・ウイルス対策を支援する統合型のエンドポイント管理ツール



On-premises LANSCOPE Endpoint Manager

- 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
- 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

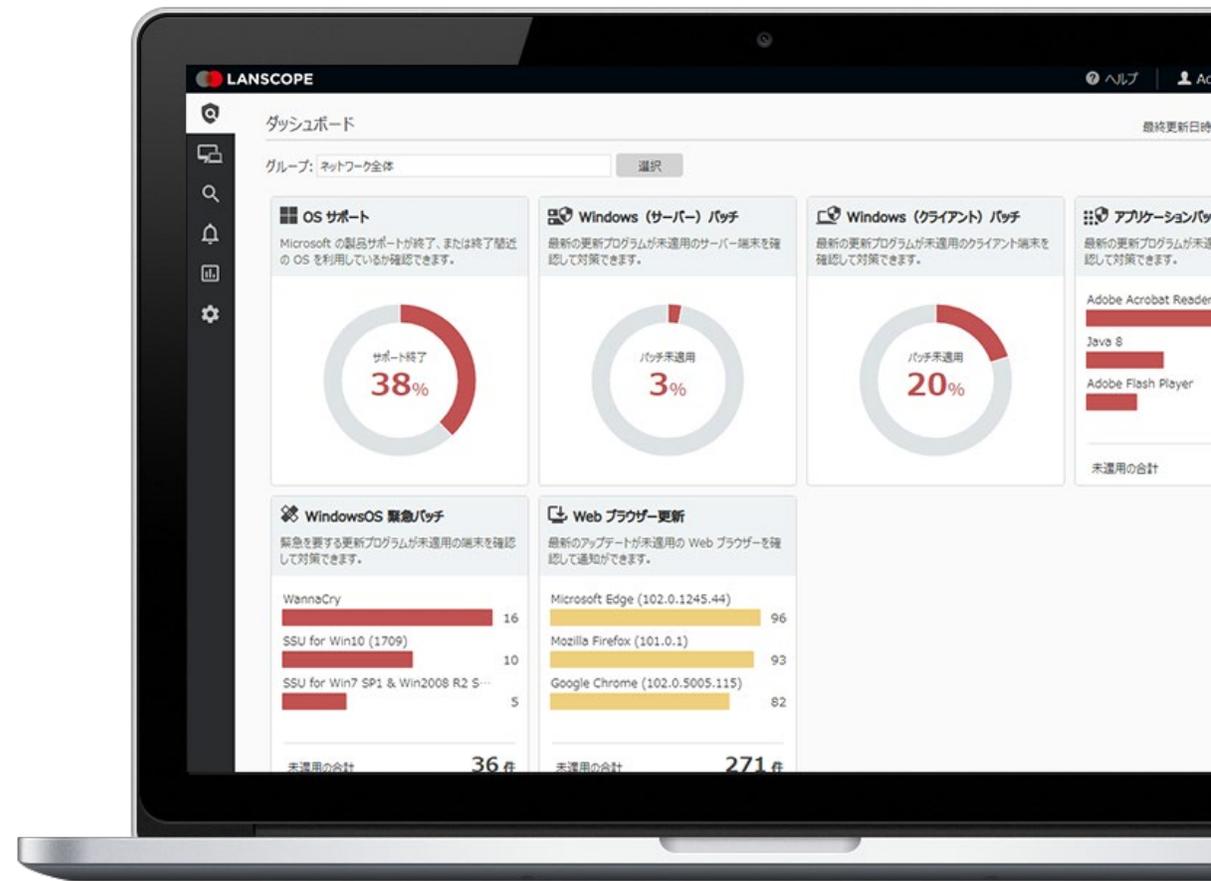
Webアクセス制御

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/>





体験版
お試し限定

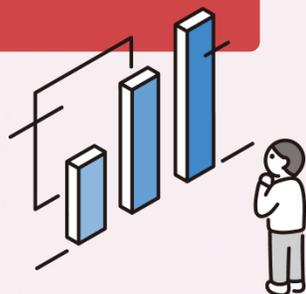
今だけ
レポートサービス
実施中

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 エンドポイントマネージャー 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。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>

未知・亜種のマルウェアもマシンラーニングで99%※検知！次世代のアンチウイルス



CylancePROTECT®

AIを活用したマシンラーニングによる予測検知が可能で、未知・亜種のマルウェアも99%の高検知が実現。LANSCOPE エンドポイントマネージャーとの連携で簡易EDR、オプションのOPTICSによるEDRが可能

AIによる高精度な予測検知

シグニチャレスで日々のアップデート不要

過検知が少なく低負荷

<https://www.lanscope.jp/cpms/blackberryprotect/>



※2018 NSS Labs Advanced Endpoint Protection Test結果より

AIアンチウイルス無料体験実施中

～CylancePROTECTを気軽に使ってみよう～

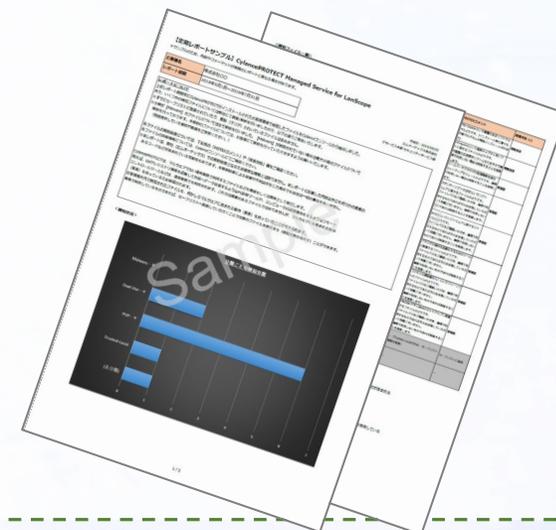
最新AIを活用した新技術で超高精度の検知率を誇る「CylancePROTECT」を**1ヶ月無料**で**何台でも体験**できるキャンペーンがスタートしました。実際に自社のPCにCylancePROTECTをインストールし、コンソールの操作方法や検知力の高さを体験いただけます。

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>



MOTEX

本資料に関するお問い合わせ

- マーケティング本部
プロダクトマーケティング部
E-mail product@motex.co.jp

ご購入後の製品利用に関するお問い合わせ

- サポートセンター 0120-968995（携帯・PHSからは06-6308-8981）
お電話受付時間 9:30～12:00/13:00～17:30（平日、祝祭日除く）
Email お問い合わせ support@motex.co.jp

本資料は厚生労働省「医療情報システムの安全管理に関するガイドライン5.2版」に基づいて作成しています。

あくまで抜粋版となりますので、正式版をご参照し、企業に合わせた対応をしていただくことを推奨します。

医療情報システムの安全管理に関するガイドライン5.2版：<https://www.mhlw.go.jp/content/10808000/000936160.pdf>

・記載の会社名および製品名・サービス名は、各社の商標または登録商標です。

・MOTEX はエムオーテックス株式会社の略称です。