徳島県医療機関向け
サイバーセキュリティ対策マニュアル
病院システム管理者向け

徳島県　保健福祉部　医療政策課

目次

- サイバーセキュリティ対策マニュアルの使い方
- サイバーセキュリティチェックリスト
- サイバーセキュリティ対策マニュアル
- 付録

サイバーセキュリティ対策マニュアルの使い方

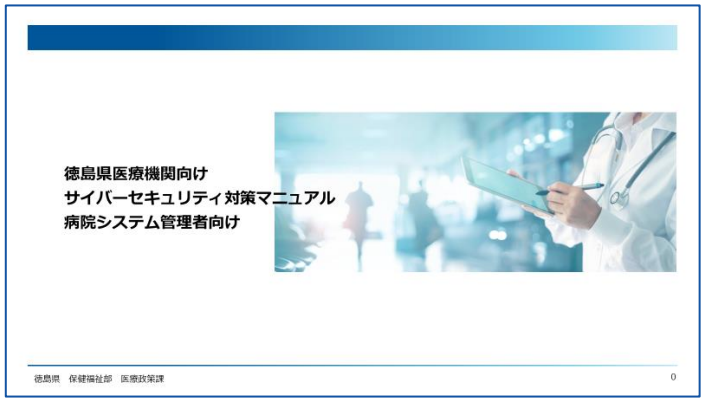
マニュアルの使い方

当マニュアルは、徳島県内の医療機関において、サイバーセキュリティ対策の現状レベルを理解し、適切な対策実施や取り組みに必要な手順を示しています。

マニュアル利用の流れ

1. 「サイバーセキュリティ対策チェックリスト」を使って、サイバー攻撃のリスクに対する現状の対策レベルを判定します。
2. 対策が不十分な項目については、「サイバーセキュリティ対策マニュアル」の該当ページを閲覧し、サイバー攻撃のリスクと対策案を確認します。
3. 「サイバーセキュリティ対策マニュアル」の対策案を参考に、医療情報システムのベンダーや保守事業者などと協力して、対策を実施します。
4. 定期的に（例えば月に1回など）、対策状況を確認するために「サイバーセキュリティ対策チェックリスト」を使用します。

No	チェック項目	結果	レベル判定				備考
			0	1	2	3	
1	サイバーセキュリティにかかる最新動向（インシデント情報やセキュリティ専門知識を持つ者等からの情報発信等）の収集を実施していますか。 医療情報システムベンダ及びサービス事業者から技術的対策や医療情報システムのアップデート等の情報を収集していますか。	0	サイバーセキュリティにかかる情報は、収集していない。	サイバーセキュリティにかかる情報を収集している。	収集した情報を基にサイバーセキュリティ対策の実施について、医療情報システムベンダ等に相談し、対応している。	医療情報システムベンダ等とサイバーセキュリティ対策に関する契約を締結している。	01.サイバーセキュリティに関する情報収集
2	医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）は、最新の状態を維持していますか。新設したインターネット回線やVPN 機器等は記載されていますか。	2	ネットワーク・システムの構成を把握していない。	ネットワーク・システムの構成の概要がわかる。	ネットワーク・システムの詳細な構成図が作成されている。	新規導入した回線や医療機器等も構成図に反映され、現状を把握できている。または、把握できるように部門間でも連携がとれている。	02.ネットワーク・システム構成の把握
…	…	…	…	…	…	…	…



サイバーセキュリティ対策チェックリストの使い方（1/2）

「サイバーセキュリティ対策チェックリスト」を使用して、現状のレベルを判定します。

No	チェック項目	結果	レベル判定（0～３）	マニュアル記載箇所
１～２０の通し番号	現場で定期的にチェックする内容	チェック項目における現在の対策レベルの判定結果を記入する（0～3の数値を記入）	チェック項目における対策状況のレベルの判定基準	対策を進めるために参照するマニュアル

レベル	現在の対策状況の判定基準
0	対策／取組みができていない状態。
1	最低限の対策／取組みができている状態。
2	基本的な対策／取組みができている状態。
3	システムの導入／契約による対策ができている状態。

サイバーセキュリティ対策チェックリストの使い方（2/2）

サイバーセキュリティ対策に必要なチェック項目を確認する。

レベル判定の項目を確認し、現在の状況に当てはまるレベルを結果欄に記入する。
基本的な対策／取組みができている状態（レベル２）となるように対策を実施する。

チェック項目に該当するマニュアルを確認する

No	チェック項目	結果	レベル判定				マニュアル記載箇所
			0	1	2	3	
1	サイバーセキュリティにかかる最新動向（インシデント情報やセキュリティ専門知識を持つ者等からの情報発信等）の収集を実施していますか。 医療情報システムベンダ及びサービス事業者から技術的対策や医療情報システムのアップデート等の情報を収集していますか。	0	サイバーセキュリティにかかる情報は、収集していない。	サイバーセキュリティにかかる情報を収集している。	収集した情報を基にサイバーセキュリティ対策の実施について、医療情報システムベンダ等に相談し、対応している。	医療情報システムベンダ等とサイバーセキュリティ対策に関する契約を締結している。	01.サイバーセキュリティに関する情報収集
2	医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）は、最新の状態を維持していますか。新設したインターネット回線やVPN 機器等は記載されていますか。	2	ネットワーク・システムの構成を把握していない。	ネットワーク・システムの構成の概要がわかる。	ネットワーク・システムの詳細な構成図が作成されている。	新規導入した回線や医療機器等も構成図に反映され、現状を把握できている。または、把握できるように部門間でも連携がとれている。	02.ネットワーク・システム構成の把握
…	…	…	…	…	…	…	…

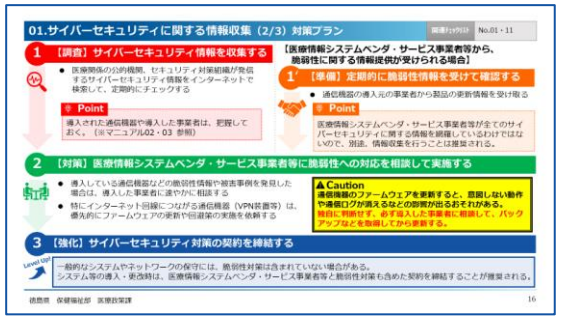
マニュアルの構成

近年の医療機関で発生しているサイバーセキュリティインシデント及び医療機関の対策の現状を踏まえ、インシデントの予防、検知、対応、復旧を行うために必要な12項目の対策について解説しています。

01.サイバーセキュリティに関する情報収集
02.ネットワーク・システム構成の把握
03.インシデントの早期対応
04.オフラインバックアップの実施
05.医療情報システムへのアクセス管理
06.保守作業等の医療情報システムへのアクセス管理
07.アクセスログの取得と不審なログの確認
08.ウイルス対策ソフトの管理
09. OSのセキュリティ・パッチ適用
10.情報機器・記録媒体の持ち込み管理
11.情報機器・記録媒体の持ち出し管理
12.インターネット・電子メールの取り扱いの注意

【各項目の解説ページ構成】

1.想定されるリスクとその対策案をまとめた概要ページ



2.対策案の準備、実施及び強化するプランを示すページ

3.具体的に対策を実施するための方法の一例を紹介するページ（付録の活用方法を含む）

サイバーセキュリティチェックリスト

No	チェック項目	結果	備考
1	サイバーセキュリティにかかる最新動向（インシデント情報やセキュリティ専門知識を持つ者等からの情報発信等）の収集を実施していますか。医療情報システムベンダ及びサービス事業者から技術的対策や医療情報システムのアップデート等の情報を収集していますか。		01.サイバーセキュリティに関する情報収集
2	医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）は、最新の状態を維持していますか。新設したインターネット回線やVPN機器等は記載されていますか。		02.ネットワーク・システム構成の把握
3	医療情報システムに関するシステム責任者一覧（設置事業者等含む）は、最新の状態を維持していますか。		03.インシデントの早期対応
4	バックアップは、正常に取得できていますか。バックアップの一部は、オフラインバックになっていますか。		04.オフラインバックアップの実施
5	医療情報システムへのアクセスにおける利用者は、契約終了等に合わせて、アクセス権限を無効化していますか。		05.医療情報システムへのアクセス管理

No	チェック項目	結果	備考
6	医療情報システムへのアクセスにおける利用者は、人事異動等による利用者の担当業務の変更等に合わせて、アクセス権限の変更を行っていますか。		05.医療情報システムへのアクセス管理
7	アクセスログは取得できていますか。大量のログイン失敗の形跡等の不審なログはありませんか。		07.アクセスログの取得と不審なログの確認
8	医療情報システムの時刻は合っていますか。		07.アクセスログの取得と不審なログの確認
9	ウイルス対策ソフトのパターンファイルは更新されていますか。		08.ウイルス対策ソフトの管理
10	OSのセキュリティ・パッチを適用していますか。		09. OSのセキュリティ・パッチ適用

No	チェック項目	結果	備考
11	脆弱性が検出されたネットワーク機器（VPN機器等）は、ファームウェアを更新していますか。		01.サイバーセキュリティに関する情報収集
12	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、不正ソフトウェアが混入していないか確認していますか。		10.情報機器・記録媒体の持ち込み管理
13	保守作業等の医療情報システムに直接アクセスする作業の際には、作業者、作業内容及び作業結果を確認していますか。リモートから保守作業を行われた場合も同様に確認できていますか。		06.保守作業等の医療情報システムへのアクセス管理
14	外部に持ち出す情報機器（ノートパソコン、スマートフォン等）や記録媒体（USBメモリ等）の管理を実施していますか。		11.情報機器・記録媒体の持ち出し管理
15	職員が個人のUSBメモリ等の許可していない外部媒体を使用していませんか。		10.情報機器・記録媒体の持ち込み管理

No	チェック項目	結果	備考
16	職員が業務に関係がないウェブサイトを閲覧していませんか。		12.インターネット・電子メールの取り扱いの注意
17	職員は、見知らぬ相手先等からの添付ファイル付きの電子メールやリンク先のクリックは注意していますか。（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等）		12.インターネット・電子メールの取り扱いの注意
18	重要情報は電子メール本文に書くのではなく、添付ファイルに書いてパスワードなどで保護していますか。なおパスワードは別手段で知らせる、あるいは事前に取り決めておく等の手法とセットで行うこと。		12.インターネット・電子メールの取り扱いの注意
19	職員は、身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理者へ連絡していますか。		03.インシデントの早期対応
20	職員は、システムの異常があった場合、院内のどこに連絡し、相談すればいいのか知っていますか。		03.インシデントの早期対応

サイバーセキュリティ対策マニュアル

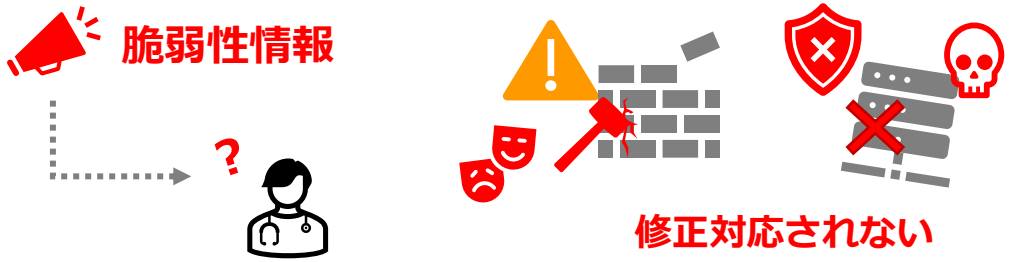
01.サイバーセキュリティに関する情報収集（1/3）概要

関連チェックリスト　No.01・11

導入している通信機器等の脆弱性（攻撃を受ける弱点）など、最新のサイバーセキュリティに関する情報を収集し、医療情報システムベンダ及びサービス事業者への対応を依頼、または定期的な確認が推奨される。

想定されるリスク

- 導入している通信機器の脆弱性に関する注意喚起がされても気が付かない
- 保守契約などがなく脆弱性の修正対応がされないまま放置される

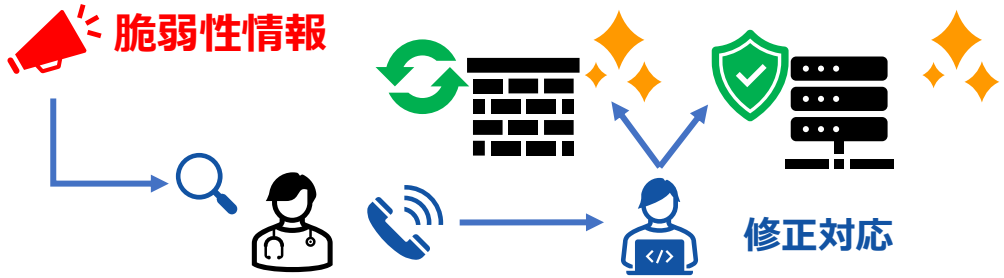


被害　脆弱性を悪用されて、院内のネットワークに侵入されたり、機密情報を窃取されたりする。

被害　対象となる機器が多く、対応に手間取る

対策案

- ✓ 院内に導入している通信機器を把握する
- ✓ 脆弱性情報を収集する
- ✓ 緊急性の高い脆弱性等は対応を依頼する



効果　最新の情報を収集して、対応の可否を判断できる

注意　インターネット回線に接続された通信機器は狙われやすいので優先的に対応する

01.サイバーセキュリティに関する情報収集（2/3）対策プラン

関連チェックリスト No.01・11

1 【調査】サイバーセキュリティ情報を収集する

- 医療関係の公的機関、セキュリティ対策組織が発信するサイバーセキュリティ情報をインターネットで検索して、定期的にチェックする

Point

導入された通信機器や導入した事業者は、把握しておく。（※マニュアル02・03 参照）

【医療情報システムベンダ・サービス事業者等から、脆弱性に関する情報提供が受けられる場合】

1′ 【準備】定期的に脆弱性情報を受けて確認する

- 通信機器の導入元の事業者から製品の更新情報を受け取る

Point

医療情報システムベンダ・サービス事業者等が全てのサイバーセキュリティに関する情報を網羅しているわけではないので、別途、情報収集を行うことは推奨される。

2 【対策】医療情報システムベンダ・サービス事業者等に脆弱性への対応を相談して実施する

- 導入している通信機器などの脆弱性情報や被害事例を発見した場合は、導入した事業者に速やかに相談する
- 特にインターネット回線につながる通信機器（VPN装置等）は、優先的にファームウェアの更新や回避策の実施を依頼する

⚠ Caution

通信機器のファームウェアを更新すると、意図しない動作や通信ログが消えるなどの影響が出るおそれがある。
独自に判断せず、必ず導入した事業者に相談して、バックアップなどを取得してから更新する。

3 【強化】サイバーセキュリティ対策の契約を締結する

Level Up!

一般的なシステムやネットワークの保守には、脆弱性対策は含まれていない場合がある。
システム等の導入・更改時は、医療情報システムベンダ・サービス事業者等と脆弱性対策も含めた契約を締結することが推奨される。

01.サイバーセキュリティに関する情報収集（3/3）具体的な対策

関連チェックリスト No.01・11

Start!

Webサイトからサイバーセキュリティに関する情報を定期的に確認してみましょう！

Webサイト	URL	概要
Check! **厚生労働省 医療分野のサイバーセキュリティ対策について**	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html	医療関係のサイバーセキュリティに関する注意喚起、法令・ガイドライン等の対応がまとめられている。全国の医師会・医療機関に通達される情報も含まれるため、**まずはこのサイトから確認することが推奨される。**
IPA（独立行政法人 情報処理推進機構）	https://www.ipa.go.jp/security/index.html	情報セキュリティの注意喚起や啓発コンテンツなどを公開している。サイバー攻撃の相談窓口も設けられている。
JPCERT CC（コーディネーションセンター）	https://www.jpcert.or.jp/	国内で報告されたインシデント情報、製品の脆弱性情報及び詳細な対策手順がまとめられている。
Security Next（ニュースガイア株式会社）	https://www.security-next.com/	情報セキュリティに特化したニュース専門メディアサイト。最新の国内のインシデント情報がまとめられている。

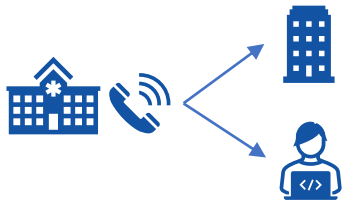
1 毎月１回、Webサイトから情報収集

導入している製品に新たな脆弱性情報が公開された

医療機関で脆弱性を悪用してサイバー攻撃事例が発生した

例：JPCERT CC：FortiOSの脆弱性（2022/12/19）

2 医療情報システムベンダ等への問い合わせ



- 製品の脆弱性対応の可否
- 脆弱性対応の懸念事項の確認
- 脆弱性の対応費用

等

Good!

医療情報システムベンダ等の定例会において確認事項とする

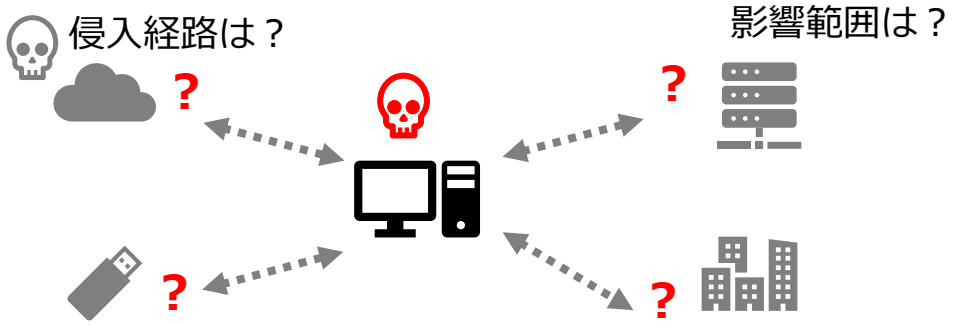
02.ネットワーク・システム構成の把握（1/3）概要

関連チェックリスト No.02

ウイルス感染などのインシデントが発生した場合、侵入経路や影響範囲などを特定して速やかに対応ができるように、院内のネットワーク、システム構成図を作成し、更新しておくことが推奨される。

想定されるリスク

- インシデント発生時に、侵入経路や影響を受けるシステムが特定できない
- システム導入時に受領した構成図から全く更新されておらず、現状に合っていない



被害

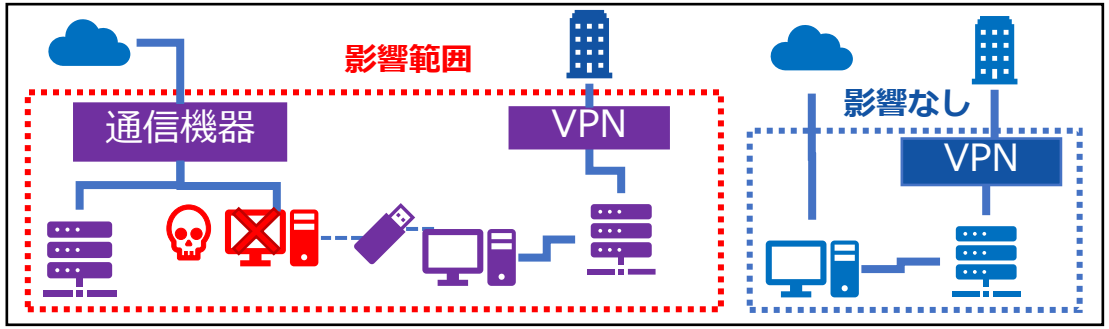
原因や影響範囲の特定に時間がかかり、インシデント対応が進まない

被害

対応漏れにより、同じ経路から侵入されて被害が再発してしまう

対策案

- ✓ 医療情報システムに関する全体構成図（ネットワーク構成図／システム構成図）を作成する
- ✓ 全体構成図を定期的に見直して、最新の状態を維持する



効果

構成図から原因や影響範囲が予測できるため、必要な対応が明確になる

注意

各部門のシステム・通信機器の導入や更改の都度、構成図を見直す必要がある

02.ネットワーク・システム構成の把握（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.02

1 【調査】ネットワーク構成の概要を整理する

- 現在のネットワーク構成の概要を整理する

Point

次のページを参照して、付録１：「ネットワーク簡易構成図」を基にネットワーク構成の概要を整理することで、対策が進めやすくなる。

【システム導入時に構成図を受領している場合】

1′ 【準備】導入時の構成図と現状の確認

- 更新日が最新の構成図を参照する
- 構成図の更新日以降に、更改・廃棄したシステムや通信機器等があれば、メンテナンス前にメモをしておく

2 【対策】全体構成図を作成する

- 整理したネットワーク構成を基に**医療情報システムベンダ等に全体構成図の作成（メンテナンス）を依頼する**
- インターネット回線・VPN通信機器・保守事業者のリモート保守回線等、外部との通信を行う装置を把握できるようにする
- 各システム間のネットワーク通信、USBメモリ等の記録媒体によるデータのやり取りも把握できるようする

Point

医療機関のネットワーク・システム構成には、ネットワーク構築事業者、医療情報システムベンダ、保守事業者等の複数の事業者が関連しているケースが多い。
回線・各種機器等を導入した全ての事業者に確認しなければ、構成図に漏れが発生するおそれがある。

3 【強化】各部門管理のネットワーク回線・医療機器・IoT機器等を全体構成図に反映する

Level Up!

各部門で個別に管理しているネットワーク回線、医療機器、ネットワークカメラ等のIoT機器は、全体構成図から漏れるおそれがある。新規導入又は廃止した回線や機器等があれば、定期的に部門間で連携を取りながら、組織全体の構成図として更新する。

02.ネットワーク・システム構成の把握（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.02

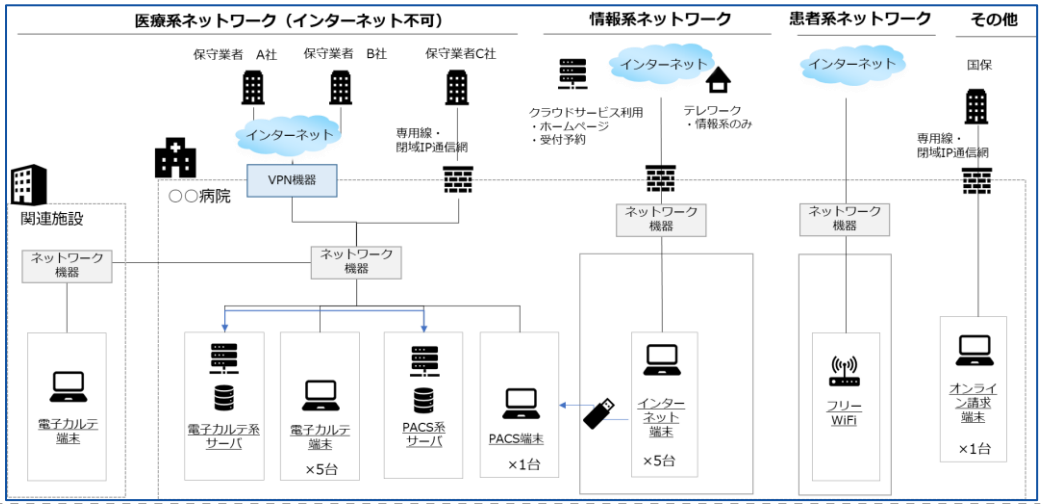
Start!

現在のネットワーク構成を整理してみましょう！

- 医療情報システムの導入時の構成図等、医療情報システムベンダ等から受領した構成図を活用する
  - 構成図が不明な場合は、**付録１：「ネットワーク簡易構成図」**を基に現在のネットワーク構成を整理する
  - 外部と接続する機器は正確に把握できるようにする
  - 保守事業者等の回線が複数あって記載できない場合は、別途保守事業者等の一覧で管理してもよい

Check!

付録１：「ネットワーク簡易構成図」



Good!

内部のデータのやり取りをわかるように構成図とネットワーク管理表等を整理しておくことが望ましい

- インシデント発生時に侵入経路の把握や接続している先がわかるように構成図とネットワーク管理表を整備する
  - パソコン、サーバ、通信機器以外にも、ネットワークに接続する医療情報機器、監視カメラ、プリンタ等も記載する

ホスト名	IPアドレス	備考
Web01	172.16.xxx.xxx	インターネット端末01
…	…	…
Med01	172.20.xxx.xxx	電子カルテ端末01
…	…	…
VPN01	10.254.xxx.xxx	VPNルータ01
FireWall01	10.254.xxx.xxx	ファイアウォール01

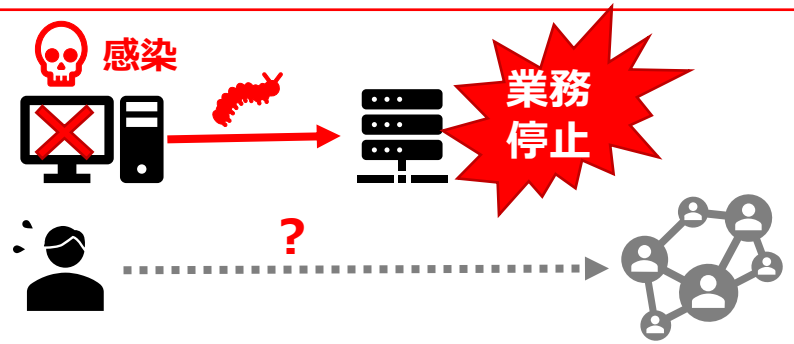
03.インシデントの早期対応（1/3）概要

関連チェックリスト　No.03、19、20

サイバー攻撃を受けた、システムに異常が発生した場合等に、初動対応が遅れると影響が広がるおそれがあるため、職員が異常を発見した時の対応を決定し、周知しておくことが推奨される。

想定されるリスク

- システム異常を見つけても、どのように対応して良いかわからず対応が遅れる
- ウイルスに感染したパソコンがネットワークに接続されたまま放置されると、感染が拡大する

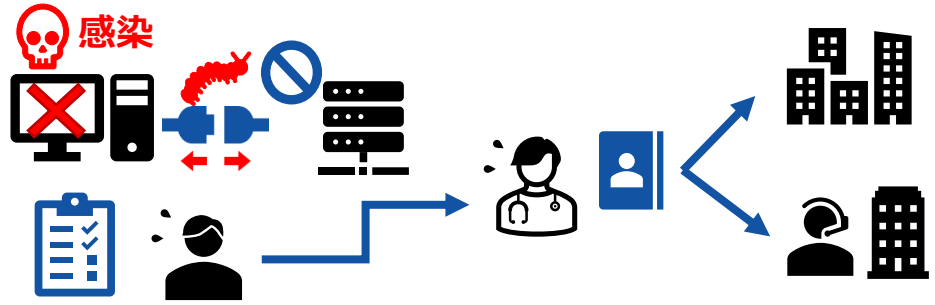


被害　**対応が遅れることで影響が広がり、収拾がつかなくなる**

被害　**現場で誤った対応をしてしまい状況が悪化する**

対策案

- ✓ 現場で異常を検知した時に連絡する窓口を決めて、連絡が必要なことを周知する
- ✓ 異常時の対応チェックリストを配布し、被害を少なくする措置ができるように備える



効果　**現場が速やかに適切な対応をすることで、被害が最小限に抑えられる**

注意　**適切に対応できるように、定期的な注意喚起、教育訓練が必要**

03.インシデントの早期対応（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.03、19、20

1 【準備】責任者を決定して文書化する

- 医療情報システムの責任者を決定する
- 責任者・連絡先を文書化する
  - ➢ **付録２：「サイバーセキュリティ体制図」、付録３：「外部連絡先一覧」**などを基に作成する

Point

インシデントが発生した際の報告漏れを防ぐため、**報告が必要な外部機関や医療情報システムベンダの担当者の連絡先なども整理しておく。**

2 【対策】対応方法を現場に周知する

- 責任者にはインシデント対応の必要性を認識させる
  - ➢ **別紙「インシデントチェックリスト」を責任者に配布する**
- 職員向けにインシデント発生時の注意喚起をする
  - ➢ **付録４：「サイバーセキュリティ対策5ヶ条」を、職員が参照しやすい場所に掲示する**
  - ➢ 緊急事態に速やかにシステム責任者の連絡先を参照できるようにしておく

⚠ Caution

患者の健康情報等の要配慮個人情報は、1件でも漏えい・滅失・毀損が発生した、またはその疑いがある場合、個人情報保護委員会または関係省庁への報告及び本人への通知義務がある。
インシデント対応には、法令上の義務が含まれることを認識しておく。

3 【強化】定期的な訓練を実施する

Level Up!

文書を作成して周知しただけでは、対応が認識されないおそれがある。サイバーセキュリティの専門機関が行う教育サービスなどを活用して、サイバーセキュリティの集合教育、標的型メール訓練など、少なくとも年に１回は教育訓練を実施する。

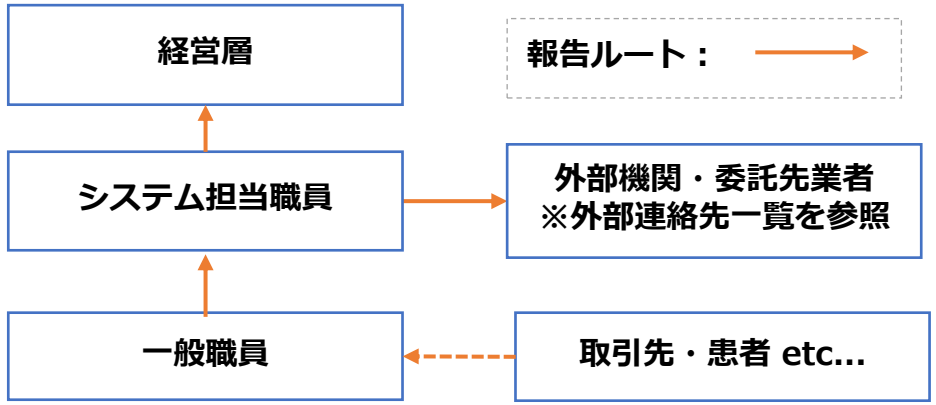
03.インシデントの早期対応（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.03、19、20

Start!

インシデント対応の体制を整備して文書化しましょう！

- システム担当となる職員を明確にして、誰から誰に報告するかわかるようにする
- 既存の組織体制図、連絡網などを活用してもよい



Check!

付録２：「サイバーセキュリティ体制図」

Check!

付録３：「外部連絡先一覧」

- 厚生労働省、IPA、個人情報保護委員会など報告・相談が必要な連絡先はあらかじめ、とりまとめてある
- 医療情報システムベンダ、保守事業者等の連絡先を追加して、整備する

項番	組織名	電話番号・FAX・URL	メールアドレス	備考
1	厚生労働省 医政局特定医薬品開発支援・医療情報担当参事官室	TEL：03-6812-7837	igishitsu@mhlw.go.jp	サイバー攻撃を受けた場合の厚生労働省の連絡先
2	一般社団法人　ソフトウェア協会（厚生労働省委託事業） 医療機関向け　セキュリティ教育支援ポータルサイト	https://mhlw-training.saj.or.jp/incident/	―	医療機関において、セキュリティインシデントの疑いがある内容について、問い合わせができる ※重大なインシデントを除き、厚生労働省への情報共有は行われない
3	独立行政法人情報処理推進機構(IPA) 情報セキュリティ安心相談窓口	TEL：03-5978-7509 FAX：03-5978-7518	anshin@ipa.go.jp	ウイルス感染、不正アクセスが発生した場合などは連絡する
4	独立行政法人情報処理推進機構(IPA) サイバーセキュリティお助け隊サービス	https://www.ipa.go.jp/security/otasuketai-pr/	―	監視システムの導入支援などが受けられる
5	個人情報保護委員会	https://www.ppc.go.jp/legal/rouei/	―	個人情報を含むデータの漏洩、滅失、毀損が発生した場合（不正アクセス等を含む）は連絡
6	徳島県庁　保健福祉部　医療政策課	TEL：088-621-2366	iryouseisakuka@pref.tokushima.jp	県への報告・相談
7	徳島県警察 サイバー犯罪に関する相談及び情報	TEL：088-622-3180	―	フィッシング詐欺、ウイルス等の被害にあった場合は連絡する
8	例：電子カルテベンダ ○○株式会社　○○部　○○様	088-●●●-●●●	○○@○○.co.jp	電子カルテシステムの障害発生時に連絡

【参考】サイバーセキュリティ対策の教材

Level Up!

サイバーセキュリティの教育訓練には教材を活用しよう！

Check!

医療機関向けセキュリティ教育支援ポータルサイト（厚生労働省）

https://mhlw-training.saj.or.jp/

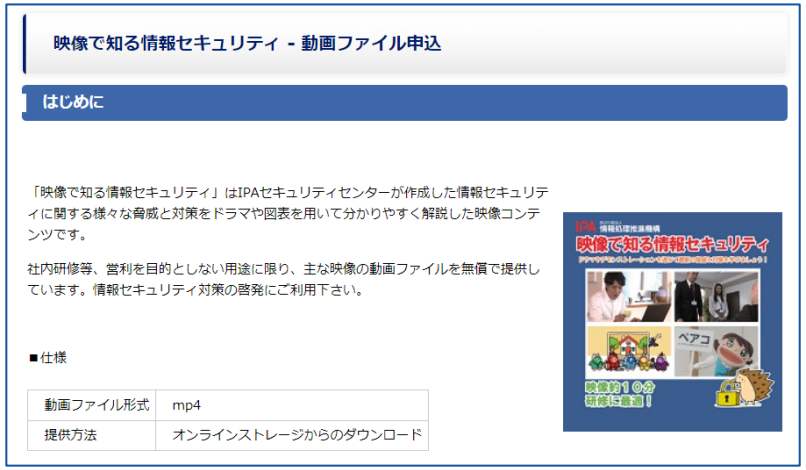
- 医療機関向けに無料のオンライン研修などを提供されている
  ※申し込みが必要な講座もある
- システム・セキュリティ管理者向け、初学者・医療従事者向けなど立場によってメニューが分かれている

Check!

映像で知る情報セキュリティ（IPA 情報処理推進機構）

https://www.ipa.go.jp/security/keihatsu/videos/

- 情報セキュリティに関する様々な脅威と対策をドラマや図表を用いて分かりやすく解説したコンテンツ
- 職場内の研修などであれば、動画ファイルが無償で提供されている
- インターネット環境であれば、動画配信サイトによるコンテンツ動画の配信も行われている



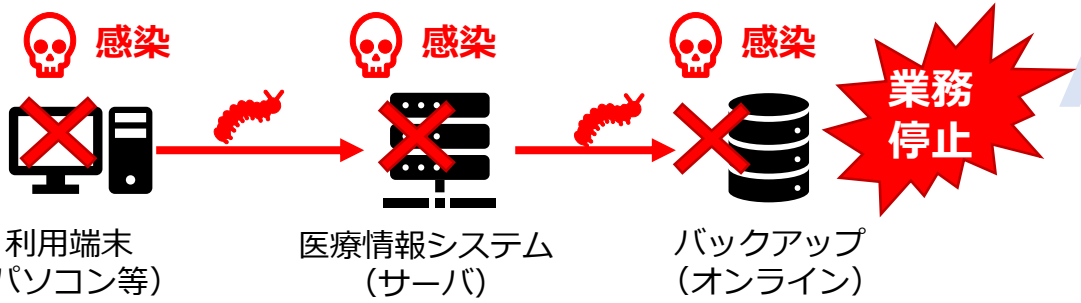
04.オフラインバックアップの実施（1/3）概要

関連チェックリスト No.04

医療情報システムのバックアップデータは、院内のネットワーク（オンライン）だけでなく、物理的（または論理的）に切り離された環境（オフライン）にも取得して、管理することが推奨される。

想定されるリスク

- 医療情報システムがランサムウェアに感染する
- ネットワークを経由して、バックアップデータまで感染が拡大し、復旧ができなくなる

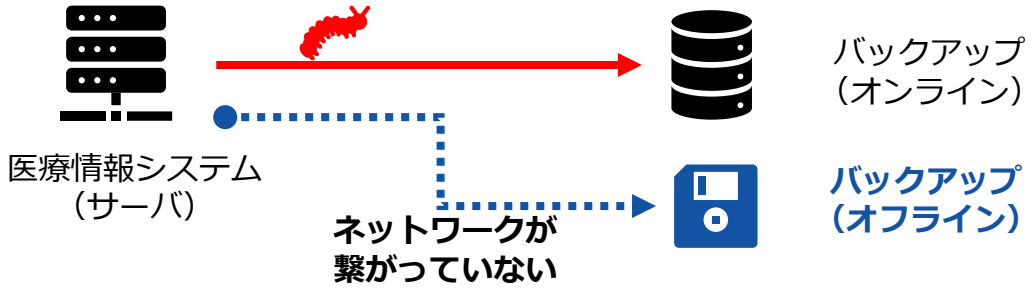


被害 **医療情報が完全に失われてしまう**
（身代金を支払っても復旧できる保証はない）

被害 **業務復旧に膨大なコスト（お金・時間）がかかる**

対策案

- ✓ バックアップデータのオフライン保管を実施する
- ✓ 定期的に、バックアップデータが正常に取得され、保管されていることを確認する



効果 **ランサムウェアの感染が拡大しても、最低限のコストで業務復旧ができる**

注意 **バックアップ未実施のシステムが無いように定期的に取得する必要がある**

04.オフラインバックアップの実施（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.04

1 【準備】オフラインバックアップを計画する

- バックアップを取得するシステムを検討する
  - ➢ システムが停止することによる業務への影響が大きいシステムから優先的に行う
- **医療情報システムベンダ等にオフラインバックアップの取得方法を相談する**
- 検討結果を基にバックアップの環境を準備する

Point

バックアップ容量、世代、記録媒体などの要件を認識してバックアップの方法を検討する

⚠ Caution

バックアップから正常に復旧するために、システム障害時における復旧対応の契約を、医療情報システムベンダ等と締結する事が推奨される

2 【対策】オフラインバックアップを実施する

- 院内でバックアップを運用する場合、担当者、実施手順を決定して、システム利用時間外に取得する
- 定期的にバックアップを取得できていることをチェックリスト等で確認する

⚠ Caution

バックアップした媒体は、重要な医療情報を含むため、必ず施錠できる場所に保管して、システム管理者やバックアップの担当者以外が持ち出せないように管理する

3 【強化】定期的にバックアップ状況を管理する

Level Up!

容量不足によるバックアップの失敗や媒体の劣化による破損などのおそれがあるため、バックアップの取得状況を確認する。
オフラインバックアップ媒体から、復元ができるかテストを実施する。

04.オフラインバックアップの実施（3/3）具体的な対策

関連チェックリスト No.04

Start!

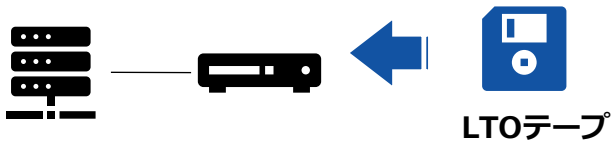
オフラインバックアップの方法を検討しましょう！

オフラインバックアップの方法は、必ず医療情報システムベンダに相談してから決定する。
簡易的な実施方法は以下の通り。

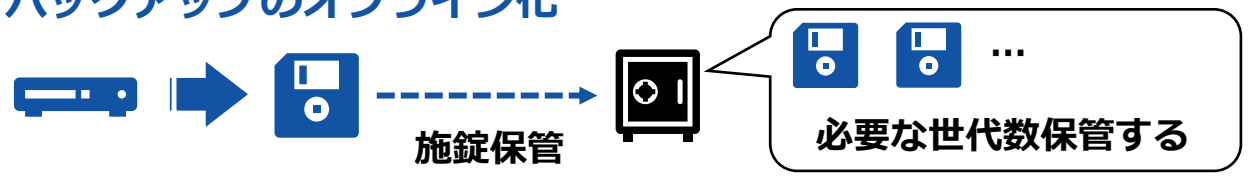
Check!

実施例①　LTOテープによるバックアップ

1 バックアップの実施



2 バックアップのオフライン化

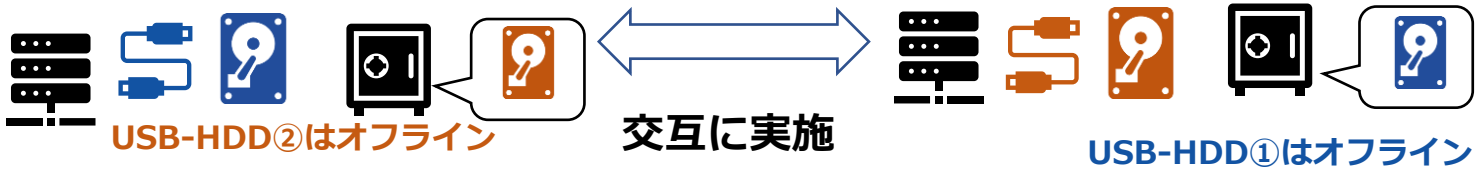


Check!

実施例②　2台以上のUSB-HDD（ハードディスク）によるバックアップ

1 ２台以上のUSB-HDDを準備

2 USB-HDDを入れ替えながらオフラインバックアップの実施



【その他のオフラインバックアップについての補足】

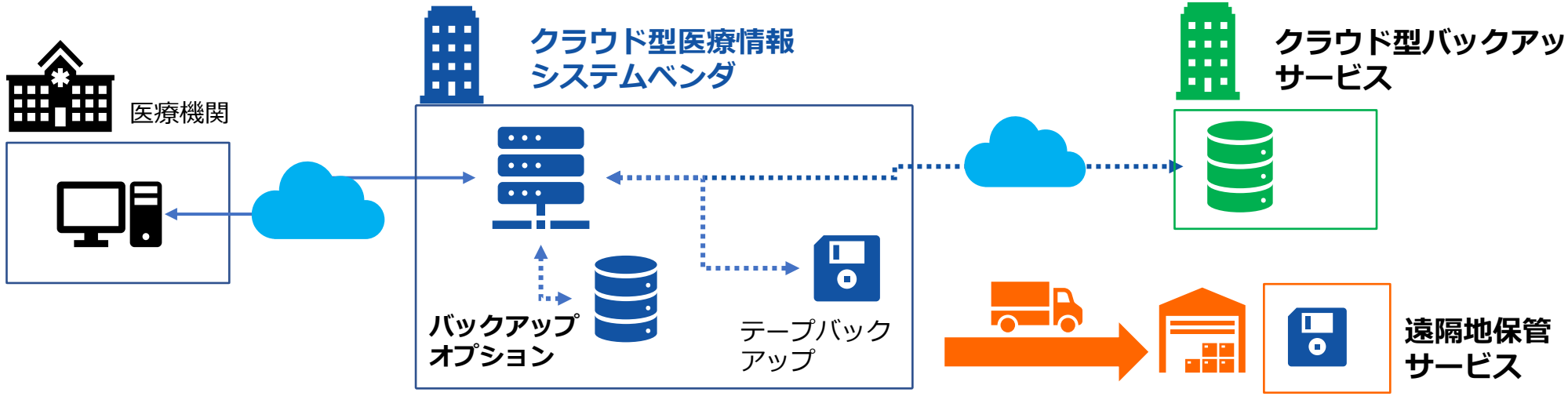
- 一度データを保存すると再書き込みが不可能となる媒体にであれば、接続したままでもよい
- イメージバックアップを取得しておくことで、復旧時間を短縮することができる

【参考】クラウドサービス型の医療情報システムを利用する場合

関連チェックリスト No.04

Level Up!

クラウド型の医療情報システムはバックアップサービスを利用する



【バックアップサービスの確認事項】

- サービス仕様書を確認し、バックアップの取得を有効にしておく（※オプションとなっていることがある）
- オフラインバックアップに対応していることを確認する
- クラウドサービスのサーバ、バックアップの設置場所が日本国内であることに注意する
  - 国外の法令が適用されるおそれがある（外国政府による情報の徴収、検閲など）
- データ破損時に復旧対応を依頼する窓口の問い合わせ方法・時間などを把握する

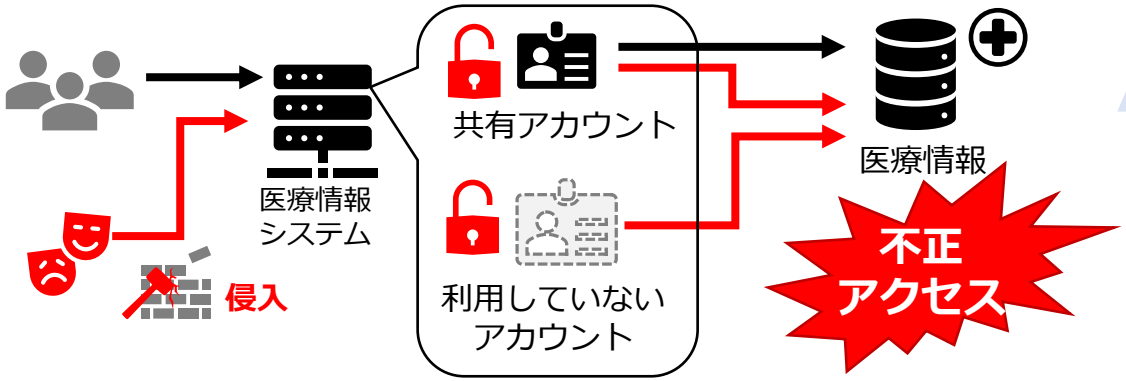
05.医療情報システムへのアクセス管理（1/3）概要

関連チェックリスト No.05、06

医療情報システムにアクセスできる者を必要最小限に制限し、利用しなくなったアカウントは速やかに無効化にすることが推奨される。

想定されるリスク

- ✓ 医療情報システムのアクセス権限が分かれていない
- ✓ 簡易なパスワードが設定されている
- ✓ 利用していないアカウントが不正に使用される

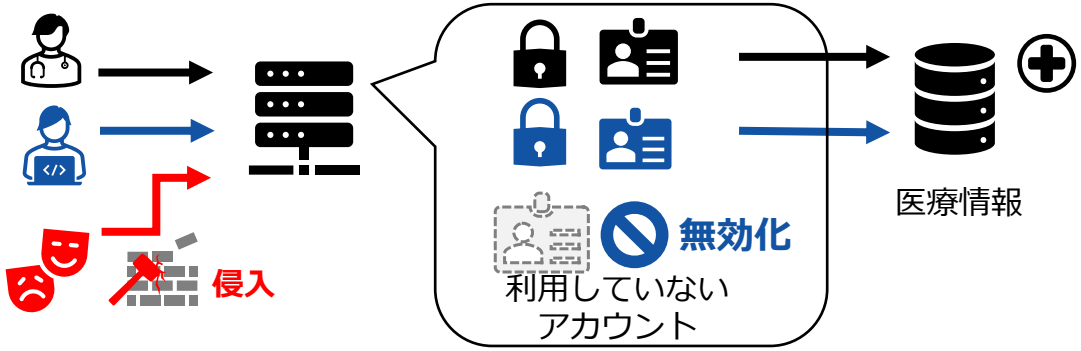


被害

攻撃者に院内のネットワークに侵入されると、アカウントが悪用されて、医療情報にアクセスされてしまう

対策案

- ✓ 業務内容、利用者・管理者の立場でアクセス権限をを分ける
- ✓ 利用していないアカウントは権限を定期的に見直し、削除または無効化する



効果

アクセスできるアカウントが限定されるため、被害が発生する可能性を低減できる

注意

アクセス権限を分けられない場合は、少なくともパソコンの認証を強化する

05.医療情報システムへのアクセス管理（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.05、06

1 【準備】医療情報システムのアクセス権限を分ける

- 原則、アカウントは共有せずに職員毎に設定する
  - ➢ 共有アカウントが必要な場合、異動、退職により共有が不要な者が発生する都度、パスワードを変更する
- 役職、部署毎にアクセスできる範囲を必要最小限にする
- パスワードは本人以外に知られないように管理する
  - ➢ 初期パスワードはアカウントの利用者本人が変更する
  - ➢ パスワードが他人に知られた場合は、速やかに変更する

Point

アカウントが不正に利用されないように、「医療情報システムの安全管理に関するガイドライン 第5.2版」においては、以下のいずれかのパスワード設定を推奨している。

- **英数字記号を混在させた13文字以上の推定困難な文字**
- **英数字記号を混在させた8文字以上の推定困難な文字＋定期的な変更（最低2か月に１度）**
- **英数字記号を混在させた8文字以上の推定困難な文字＋生体情報・ICカード等による認証（多要素認証）**

2 【対策】アクセス権限を見直す

- アクセス権限を確認して、設定を見直す
  - ➢ 退職者がいる場合は、アカウントを無効化する
  - ➢ 部署異動、昇格等により、アクセスする範囲が変わったアカウントは権限を変更する

Point

保守作業用のアカウント、システム導入時のテスト用アカウント等、登録されたまま利用していないアカウントがあれば、**保守事業者等に必要性を確認して、不要であれば無効化する**

3 【強化】アクセス権限を統合管理して、定期的に棚卸する

Level Up!

アカウントの設定状況を定期的に棚卸をして、職員のアカウントのアクセス権限を見直す。多数のパソコンのアカウントを管理する場合は、AD（Active Directory）サーバ等により、アクセス権限を統合管理することが推奨される。

05.医療情報システムへのアクセス管理（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.05、06

Start!

役職、部署ごとに必要なアクセス権限を決定しましょう！

- システムの管理者権限は特定の役職のみに割り当てる
- **攻撃者は管理者権限の窃取を狙っているため、認証を強化する**

◎：管理者（閲覧、編集、設定変更）
○：利用者（閲覧、編集）
△：閲覧者（閲覧）

役職	システム					
	電子カルテ	PACS	医事会計	放射線	…	リモート保守（VPN機器）
院長	◎	◎	◎	◎	…	-
システム管理者	◎	◎	◎	◎ ※放射線科のみ	…	-
医師	○	○	○	○ ※放射線科のみ	…	-
看護師	△	△	△	-	…	-
事務職員	-	-	○	-	…	-
保守業者	◎	◎	◎	-	…	◎

Good!

採用、異動、退職等の人事処理の一環としてアカウントの登録・変更・無効化する

- 採用、異動、退職等が発生する都度、システム管理者にアカウント設定が依頼されるように手順を定める
- アカウントの無効化・削除が困難な場合はパスワードを複雑に設定して他の人が利用できないようにする

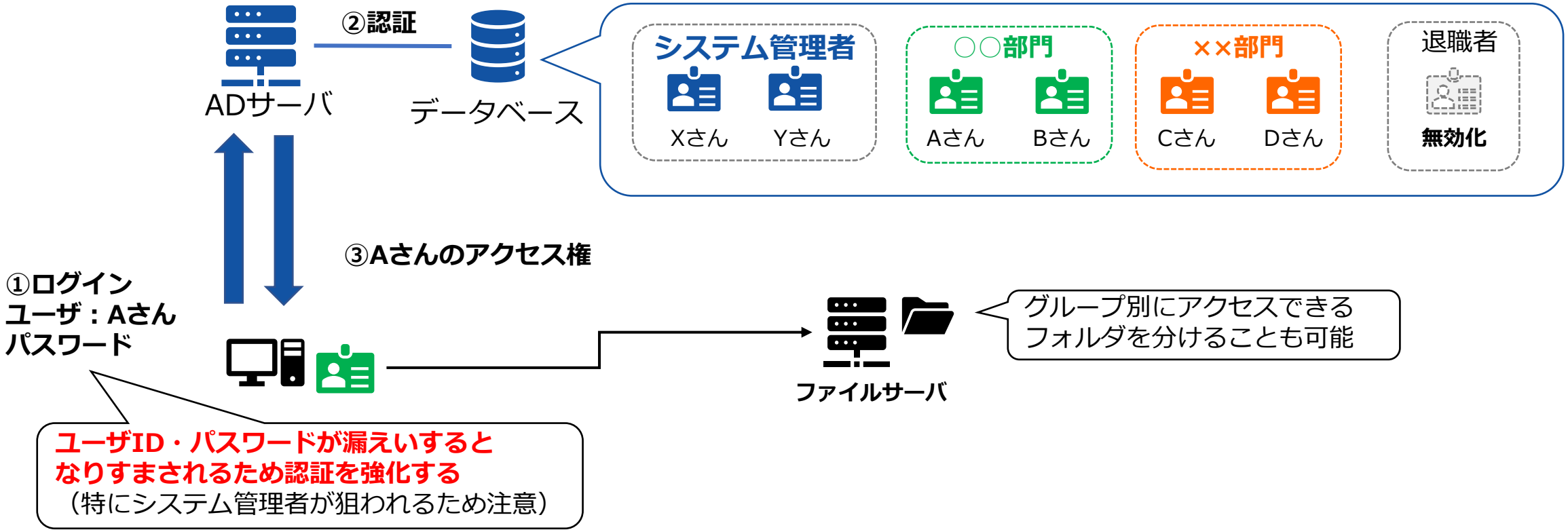
【参考】パソコン等のアクセス管理（1/2）

関連ﾁｪｯｸﾘｽﾄ No.05、06

Level Up!

ADサーバによるパソコンの統合管理

- WindowsではAD（Active Directory）サーバによって、ユーザーを統合管理する仕組みがあります。ユーザーを一元管理でき、ユーザー毎のアクセス権限やポリシー適用を実施できるので、管理する仕組みとして推奨される
- ADサーバ使用時は、不要になった職員のアカウントは、ADサーバから無効化する



【参考】パソコン等のアクセス管理（2/2）

関連ﾁｪｯｸﾘｽﾄ No.05、06

Check! 多要素認証を導入して認証を強化しよう

- ID・パスワードが知られると、本人になりすましてアカウントが不正に利用されるため、**<u>多要素認証を導入して、認証を強化する</u>**ことが推奨される
- 多要素認証とは、知識情報、所持情報、生体情報の三要素から、２つ以上の要素を組み合わせて認証する方式。
  - 例：銀行のATM　パスワード4桁（知識情報）＋　ICカード（所持情報）の二要素認証

知識情報
- ID
- パスワード
- 秘密の質問　等

＋

所持情報
- パソコン
- スマートフォン
- ICカード　等

＋

生体情報
- 指紋
- 静脈
- 虹彩　等

⚠ Caution

「医療情報システムの安全管理に関するガイドライン　第5.2版」（厚生労働省）において、令和9年度時点で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用することが求められている。

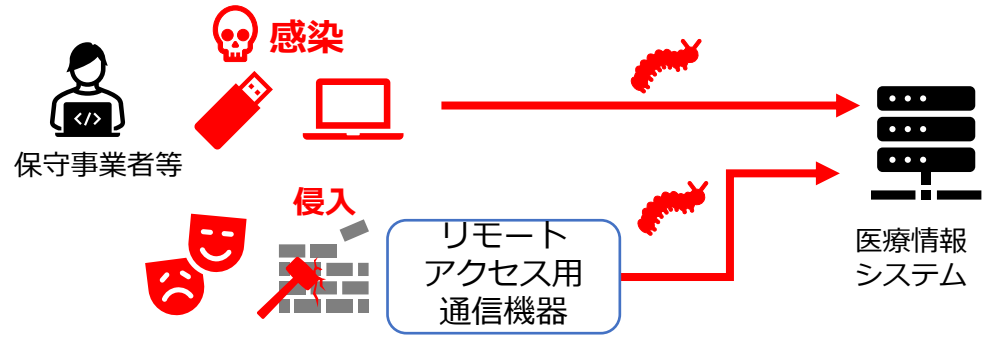
06.保守作業等の医療情報システムへのアクセス管理（1/3）概要

関連チェックリスト No.13

保守作業等により外部の者が医療情報システムにアクセスする場合は、作業内容や利用する情報機器等を把握する。また、許可された作業者以外がアクセスできないようにすることが推奨される。

想定されるリスク

- ✓ 保守作業等に持ち込まれた情報機器等にウイルスが混入している
- ✓ 保守作業等のためのリモートアクセス用通信機器に脆弱性があり、侵入される

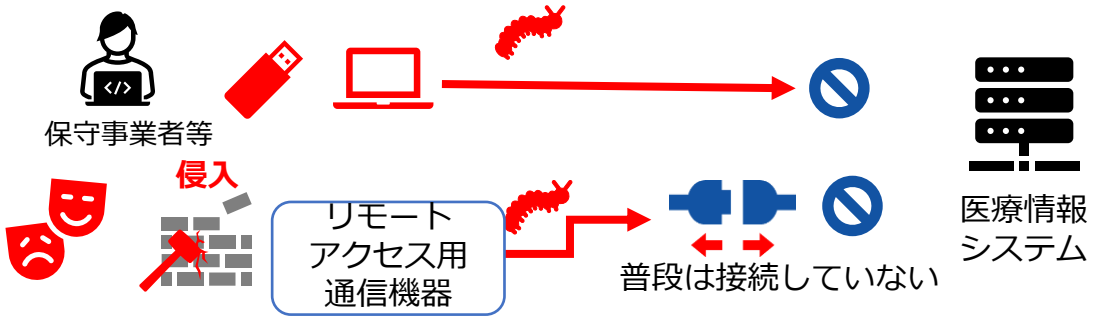


被害

保守作業に利用する情報機器やリモートアクセス用の通信回線等から、院内ネットワークに侵入される

対策案

- ✓ 医療情報システムの保守作業内容を確認する
- ✓ リモートアクセス用の通信は、アクセス時間やアクセス範囲を制限する



効果

保守作業等が原因となる被害の発生を抑止できる

注意

定期的に、許可されていない作業が行われていない事を確認する

06.保守作業等の医療情報システムへのアクセス管理（2/3）対策プラン

関連チェックリスト No.13

1 【調査】保守作業の内容を把握する

- どのような保守作業があるか保守業者に確認する
- 院内への訪問による作業の場合は、どのような情報機器、記録媒体等が持ち込まれているか確認する

Point

持ち込まれた情報機器、記録媒体はウイルスチェックなどを行う（※マニュアル10を参照）

【医療情報システムベンダ・サービス事業者等から、定例の保守作業の報告書等を受領している場合】

1′ 【調査】報告書から作業内容を把握する

- 作業日時、作業者、作業場所、作業内容を確認する
- 緊急の対応や定例以外の個別作業が発生した場合は、作業完了後に報告書が提出されていることを確認する

2 【対策】リモートアクセスの接続申請を受ける

- 保守事業者が保守作業によるリモートアクセスを行う場合は、事前に申請を受ける
- 緊急時など、事前の接続申請が困難な場合は、リモートアクセスによる作業完了後に作業報告を受ける

Point

保守作業等のアカウントが攻撃者に不正に利用されて、リモートアクセスされる事例が発生している。
インシデントが発生した場合、保守作業者のアカウントによるリモートアクセスが、保守作業等によるものか不正なものか判別できるように、リモートアクセスのログが残るように依頼する。

3 【強化】許可なくリモートアクセスができない仕組みにする

Level Up!

保守事業者のアカウントによるリモートアクセスは、保守事業者等から接続申請を受けて、医療機関側で許可した場合のみ接続できるように設計する。

06.保守作業等の医療情報システムへのアクセス管理（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.13

Start!

保守事業者の作業内容を確認しよう！

- 内容確認のため、右図のような作業申請・報告書を受領する
  - ➢次のような観点で報告書を確認する

確認項目	確認事項	注意するポイント
作業日時	● 作業を計画時の予定日時 ● システムの停止予定時間 ● 作業結果の日時	➢ 計画時と実施結果の日時の乖離があるか（理由があるか） ➢ （システムのアクセスログをチェックしている場合）ログと作業結果の日時が一致しているか
作業員	● 会社名 ● 作業者名 ● 責任者名	➢ 再委託先の作業員が行う場合は会社名が明記されているか ➢ 責任者によるチェックが実施され、作業員や再委託先等が単独で作業を行っていないか
作業場所	● 作業員が作業する場所 ● アクセス方法　など	➢ リモートアクセスの場合は、保守事業者の社内等決められた場所で行っているか
作業内容	● 作業対象となるシステム ● 作業概要（パッチ適用、バージョンアップ、設定変更等） ● 備考・連絡事項	➢ 計画外の事象やインシデントが発生していないか ➢ システムのアラートが発生する場合、保守作業の範囲外で発生していないか

作成日　20xx 年〇月△△日

作業申請書兼報告書

1. 起案

起案事項	電子カルテサーバ保守の〇月度定期メンテナンス作業の実施		
起案者		起案日	20xx 年 〇月　◇◇日

2. 作業計画（別添資料　□有り　□無し）

作業カテゴリ	■ﾊﾟｯﾁ適用　□ﾊﾞｰｼﾞｮﾝｱｯﾌﾟ　□設定変更　□その他(月次メンテナンス)
作業内容	■月次メンテナンス（リモート接続：16:00～20:30） 1．プログラム修正ファイルの適用（WindowsUpdate 等を実行）
作業対象	電子カルテシステム
作業場所	〇〇株式会社　〇階　セキュリティルーム
停止時間の有無	停止有り（18:00～20:30 間、断続的に）
利用者への通知	■実施要　□不要
作業予定日時	20xx 年 〇月△△日 16:00～21:00 （再起動等、通信に影響が出る作業は 18：00～実施予定）
計画策定者	〇〇株式会社　XX

3. 作業結果（別添資料　□有り　■無し）

作業実施日時	20xx 年 〇月△△日 16:00～20:30
作業結果	1．プログラム修正ファイルの適用（WindowsUpdate 等を実行） 対象サーバ：電子カルテシステム 〇月分のセキュリティパッチを適用 〈〈設定変更画面〉〉
作業実施担当者	〇〇株式会社　YY
ドキュメント修正	□有り（対象ドキュメント：　　）　■無し
結果確認者	〇〇株式会社　XX

4. 承認欄

処理番号	
計画承認者	
結果承認者	

5. 備考欄

【参考】保守作業によるリモートアクセスの制限

関連チェックリスト No.13

Level Up!

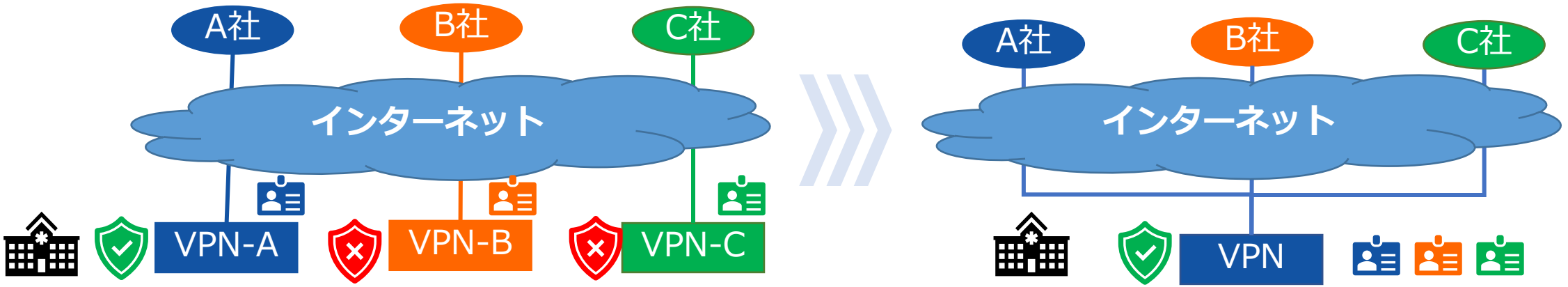
リモートアクセスによる保守作業は医療機関側で管理しよう！

- 保守作業時以外はアクセスできないようにする
  - 保守作業の担当者に変更があれば、接続するアカウントを見直す（共用の場合は、パスワードを変更する）
  - 閉域IP通信網、専用線、VPN接続により常時接続している場合は、接続できる範囲を限定する

Good!

VPN接続によるリモートアクセスを集中管理する

- 保守業者毎に個別でリモートアクセスの環境（回線、VPN機器等）を導入する場合は、管理する機器が増え、ファームウェアのアップデート漏れなどリスクが高くなる。
- 医療機関側でVPN機器を準備して、保守事業者毎にアカウントを払い出すなど、医療機関側でリモートアクセスの環境を準備して、保守業者のアクセスを集中管理する等の対策を講じる



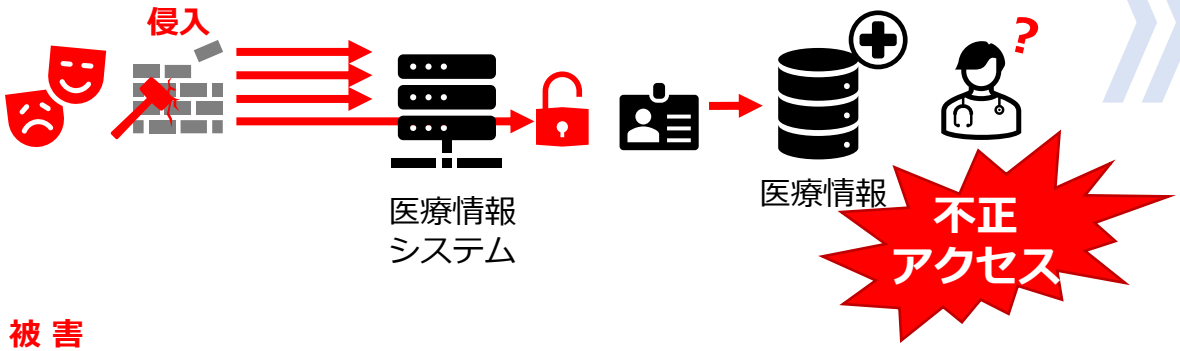
07.アクセスログの取得と不審なログの確認（1/3）概要

関連チェックリスト　No.07、08

医療情報システムのアクセスログ（接続、ログイン、操作した記録）を取得して、不審な操作や異常がないか定期的に確認することが推奨される。

想定されるリスク

- ✓ 医療情報システムのアクセスログが取得されておらず、いつ、誰がアクセスしたか、どのような操作をしたかわからない
- ✓ インシデント発生時にログの調査ができない

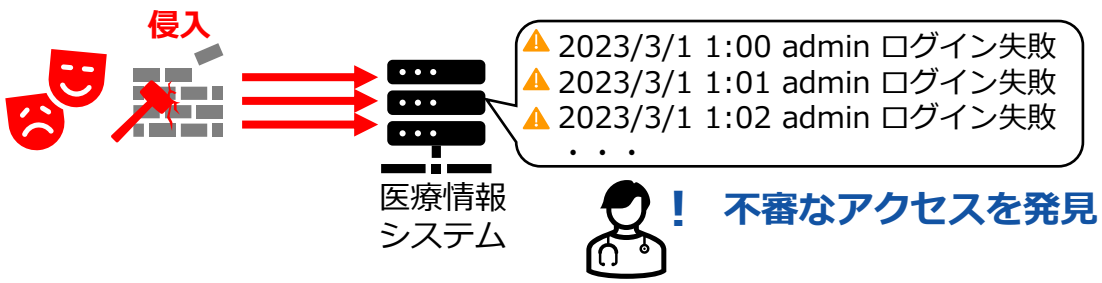


被害　インシデントが検知できず対応が遅れる

被害　インシデントが発生しても原因が特定できず対応策が立てられない

対策案

- ✓ 医療情報システムやVPN装置等のネットワーク機器のアクセスログを取得して保管する
- ✓ アクセスログが正確な時刻になっている
- ✓ 定期的にアクセスログを確認する



効果　ログを確認することで不審な操作や異常が早期発見できる

注意　医療情報システムのログと実際の時刻がずれないように時刻同期する

07.アクセスログの取得と不審なログの確認（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.07、08

1 【調査】現在のアクセスログの取得状況を医療情報システムベンダ、保守事業者等に確認する

- 利用している医療情報システム、通信機器では、どのようなログが取得できているか確認する
  - ➢ 医療情報システムの認証ログ、パソコンの認証ログ、通信ログ（リモートアクセスログ）等

Point

システムの時刻と標準時刻がずれている場合、正確な操作時間が判別できない。**ログの証拠性を確保するため、システムと標準時を同期させる必要がある。**

2 【対策】必要なアクセスログの取得を依頼する（取得を計画する）

- アクセスログの不足があれば、取得を計画する
  - ➢ 利用者のログイン時刻、アクセス時間、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
  - ➢ ログが取得できていない期間中は業務日誌等で操作者、操作内容を記録する
  - ➢ ログの保管期限を定めて、必要な容量を確保する
- 時刻のずれが発生している場合は、時刻同期する仕組みの導入を計画して実施する

⚠ Caution

インシデント対応時には、システムの調査のため、アクセスログを証跡とするが、 次のように調査ができない事象が発生している。
・ログの保管期限が短く、攻撃された時点のログが残っていない
・ファームウェアをアップデートした結果、ログが消えた　等
インシデント対応時にアクセスログが消えないように保管する方法を、計画時に決定しておくことが望まれる。

3 【強化】アクセスログを分析し、不審なアクセスがある場合は、調査を実施する

Level Up!

各種アクセスログ（Windowsログイン、リモートアクセス等）を統合管理するシステム（syslogサーバ、資産管理ツール等）を導入する。アクセスログを分析して、時間外のアクセス、大量のログインエラーなど、不審なアクセスを発見した場合は、調査する。

07.アクセスログの取得と不審なログの確認（3/3）具体的な対策

関連チェックリスト No.07、08

Start!

どのようなログがあるか確認してみよう！

医療情報システムのアクセスログ、ログイン履歴、操作履歴などから以下を確認する。

確認項目	確認事項	確認するポイント
ログイン（認証）	● ログインの成功・失敗 ● 接続元の機器の番号（IPアドレス等）	➢ 大量のログインが試されていないか ➢ 通常とは異なるパソコンから接続していないか ➢ 保守作業の時間外に保守事業者のアカウントが使われていないか
操作	● システムの参照、更新、削除 ● 設定変更（アクセス権限、パスワード）	➢ アクセスを許可していない医療情報を参照していないか ➢ 予定していない更新・削除・設定変更等を行っていないか

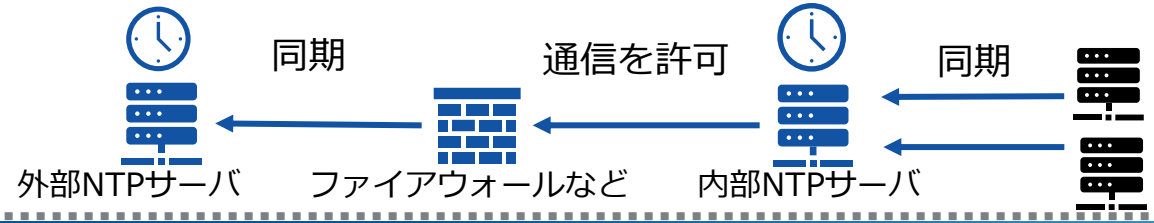
Good!

医療情報システムの時刻を自動で同期させる

インターネットに接続できない環境では、次のような仕組みを利用して、自動的に時刻同期させる

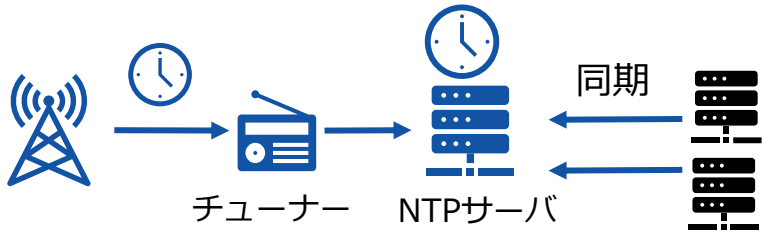
【NTPサーバの設置】

外部のNTPサーバと院内に設置したNTPサーバの通信を許可して、
時刻を同期し、院内のシステムサーバの時刻を合わせる



【FMチューナー】

FMの電波を受信して同期する

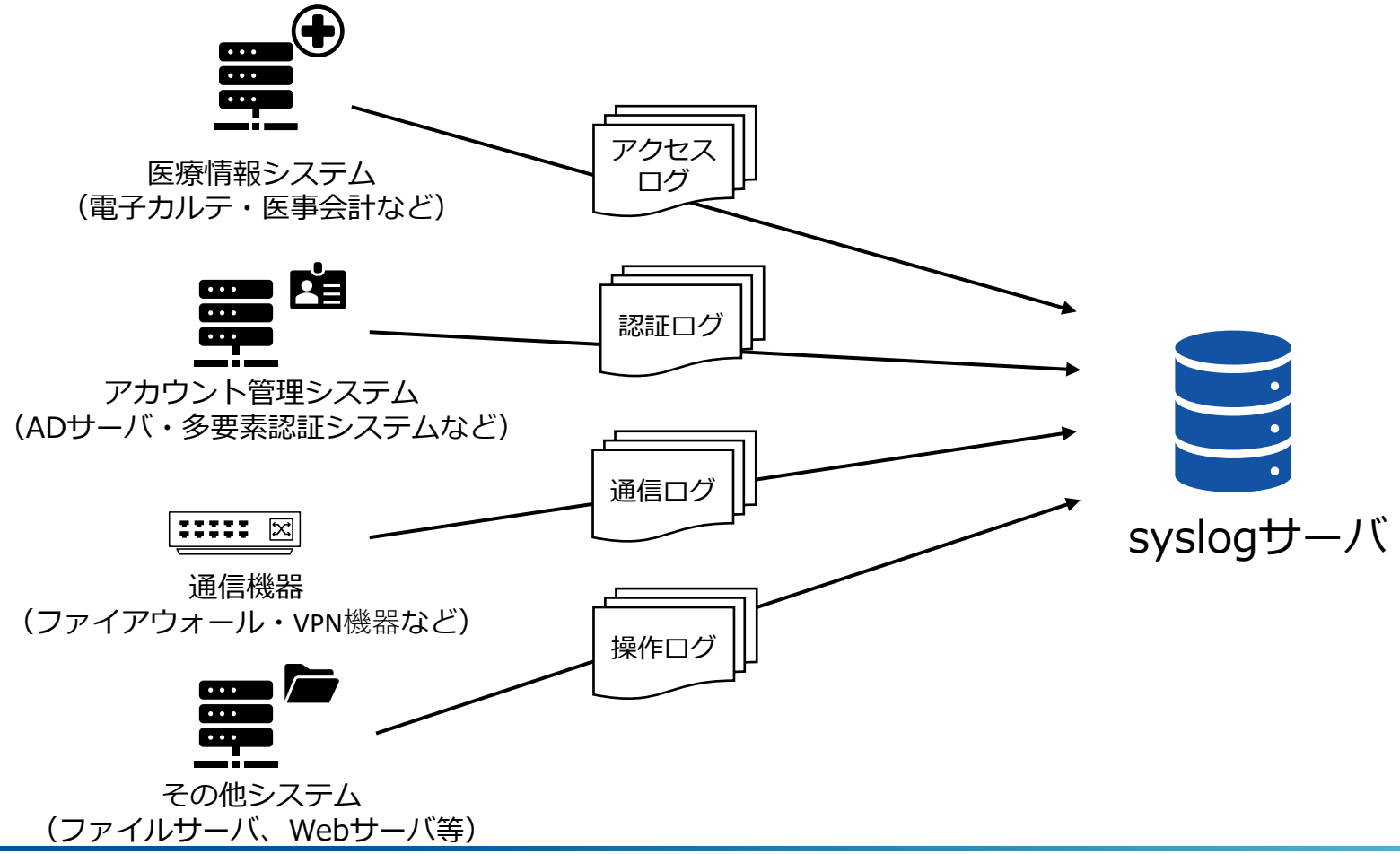


【参考】ログの統合管理

Level Up!

Syslogサーバ等の構築による複数ログの統合管理

管理するシステムが多い場合は、ログの保全、それぞれのシステムの容量の節約、ログの集約を目的に、
Syslogサーバ等を構築して、ログを統合管理することが推奨される



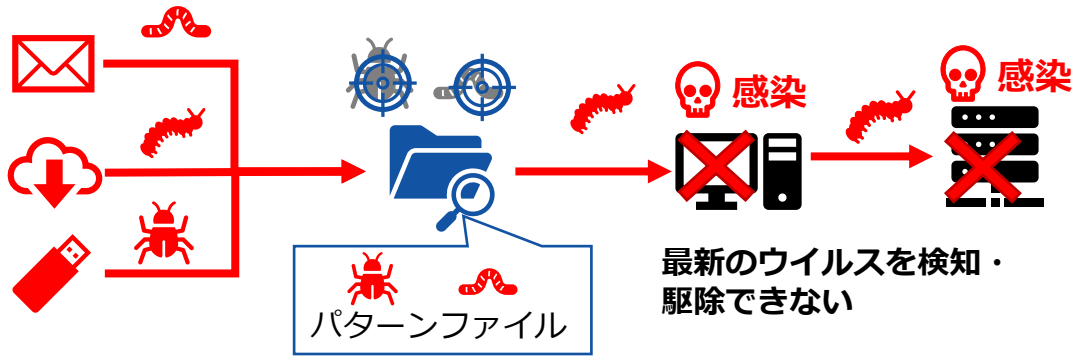
08.ウイルス対策ソフトの管理（1/3）概要

関連チェックリスト No.09

ウイルス対策ソフトのパターンファイルが古い場合、最新のウイルスを駆除できないため、定期的にパターンファイルを更新してスキャンすることが推奨される。

想定されるリスク

- ✓ 情報機器や記録媒体にウイルスが侵入してきても検知や駆除ができない
- ✓ 古いパターンファイルでは新しいウイルスは検知できない

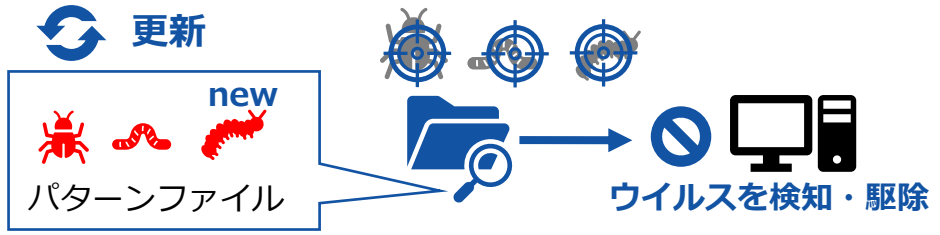


被害

ウイルスが駆除されず、院内ネットワークに拡散される

対策案

- ✓ ウイルス対策ソフトのパターンファイルを更新する
- ✓ 端末台数が多い場合は、管理システムによりウイルス対策ソフトのパターンファイルの更新漏れがないように管理する



効果

最新の状態に更新されることで、ウイルスを検知・駆除できるようになる

注意

インターネット回線に接続していない端末は、更新する方法を検討する必要がある

08.ウイルス対策ソフトの管理（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.09

1 【調査】ウイルス対策ソフトの導入状況を確認する

- 導入ができていない端末等は、ウイルス対策ソフトの導入を計画する
  - ➢ 医療情報システムのサーバにウイルス対策ソフトは、業者に確認する

Point

ウイルス対策ソフトのライセンス更新を忘れずに行う。

2 【対策】パターンファイルの更新を確認する

- ウイルス対策ソフトのパターンファイルの更新できるように設定する
- 定期的なスキャンを実施する

【ウイルス対策ソフトが導入されていない端末の場合】

※Windows10またはWindows11のパソコンの場合

1′ 【準備】OS標準のウイルス対策を活用する

- Windows Defenderを有効にする
  - ➢ 医療情報システムを利用するパソコンの場合、医療情報システムベンダに有効にしても動作上に支障がないか確認する

※Windows10またはWindows11以外の場合は、別途、ウイルス対策ソフトの導入を計画する

2 【対策】OSを更新してスキャンする

- Windows Defenderはセキュリティ・パッチを適用して、パターンファイルを更新する
  - ➢ Windows Defenderによるスキャンを定期的に実施する

3 【強化】パターンファイルの更新状況を一元管理している

Level Up!

端末の数が多い場合は、ウイルス対策ソフトの管理システム等により、パターンファイルの更新状況を一元管理する。または、クラウド型のウイルス対策ソフトを活用する。

08.ウイルス対策ソフトの管理（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.09

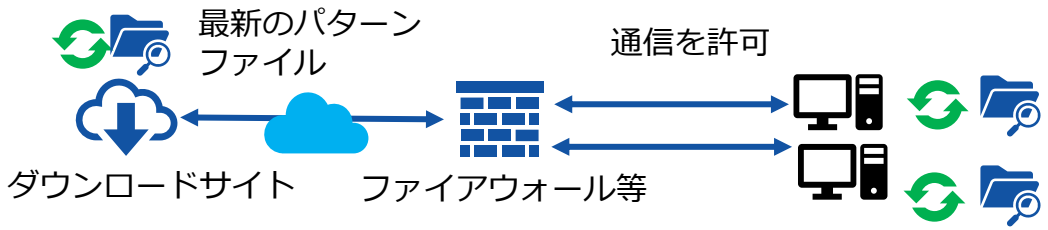
Start!

パターンファイルを更新しよう！

- インターネットに接続されていない端末等は、パターンファイルの更新ができるように対応方法を確認する

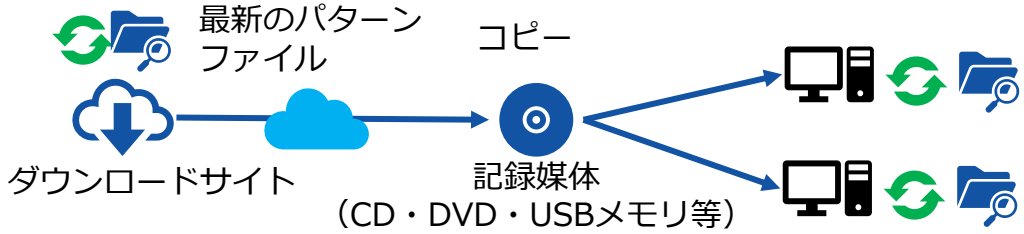
【ダウンロードサイトとの通信を許可する】

各端末とダウンロードサイトとの通信を許可して更新する



【パターンファイルを記録媒体にコピーして配布する】

定期的にパターンファイルを媒体にコピーして更新する

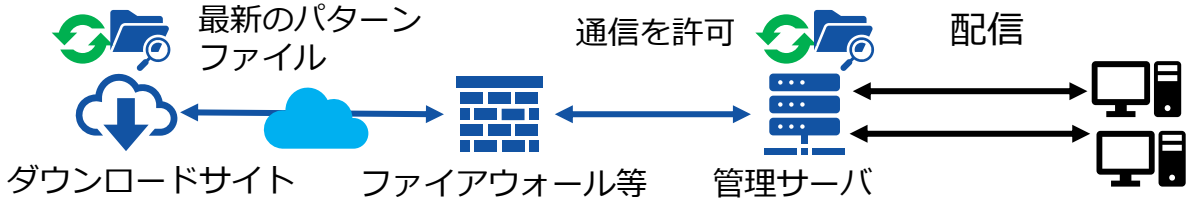


Level Up!

端末の台数が多い場合は、管理システムによりパターンファイルの更新を管理する

【管理サーバを設置する場合】

管理サーバとダウンロードサイトの通信を許可して、管理サーバから各端末に配信する



【クラウドサービス型のウイルス対策ソフトの場合】

クラウドサービス型の場合は、クラウド側にパターンファイルなどがあるため、端末とクラウドサービスとの通信を許可する

※ インターネットに接続していない場合、検知できない可能性があるため注意

【参考】EDRの導入

関連ﾁｪｯｸﾘｽﾄ No.09

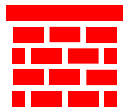
Level Up!

ウイルスが院内ネットワークに侵入することを前提としたウイルス対策を検討しよう！

- 近年はサイバー攻撃が高度化したことで、内部に侵入されて被害が発生しているため、侵入されることを前提として、侵入後の振る舞いを検知する対策が推奨される
- 侵入後の対策する仕組みとして、EDR（Endpoint　Detection and Response)の導入が必要とされている

従来のセキュリティ対策

侵入の防止



EDR（Endpoint　Detection and Response）
侵入後の動きを可視化する

検出　**隔離**　**調査**　**復旧**

Good!

EDRの導入を検討する場合は、導入後の運用も含めて必ずセキュリティ専門業者に相談する

- EDR対応の製品を導入する場合には、パソコン等の負荷が高くなるため、事前の動作検証が必要です
- EDRの導入後は、速やかな対応ができるようにSOC（Security Operation Center）等のサイバーセキュリティの専門業者等による監視サービスを利用するのが望ましい

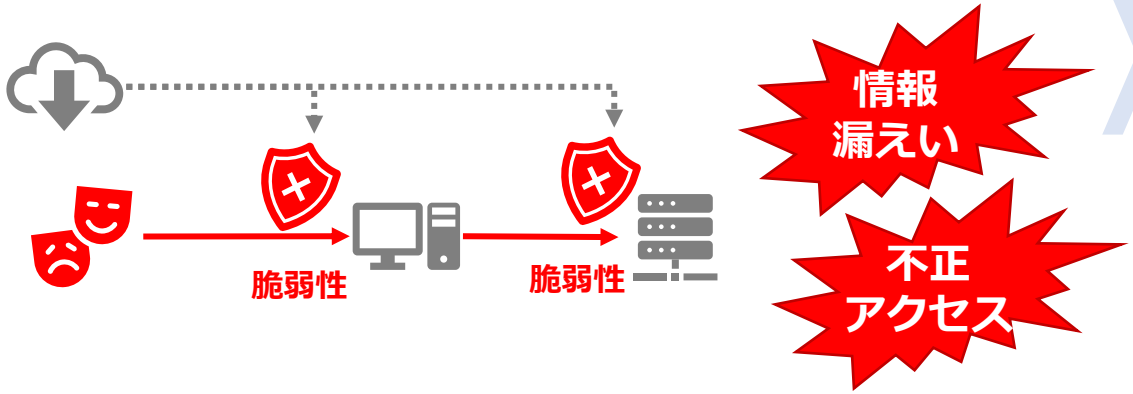
09. OSのセキュリティ・パッチ適用（1/3）概要

関連チェックリスト No.10

医療情報システムベンダの指示を受けてOS（Windowsなど）のセキュリティパッチを適用して、脆弱性を修正することが推奨される。

想定されるリスク

- ✓ 医療情報システムの機器に脆弱性が残ったままになる
- ✓ 検証していないセキュリティパッチを適用すると医療情報システムが正常に動作しなくなるおそれがある

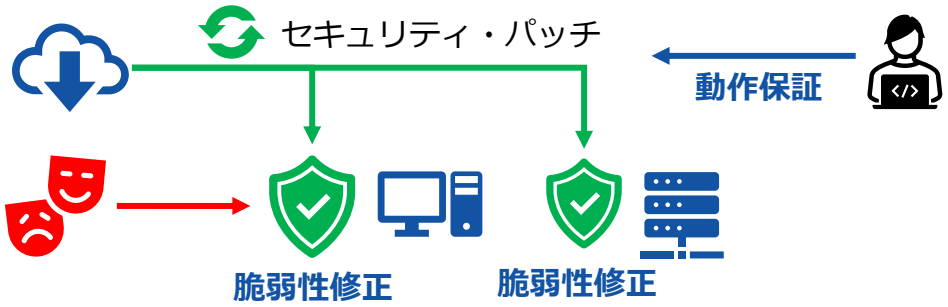


被害

OSの脆弱性が解消されず攻撃を受ける

対策案

- ✓ 医療情報システムが動作保証しているOSのバージョンを確認する
- ✓ セキュリティ・パッチの適用を計画する



効果

セキュリティ・パッチが適用され、脆弱性を修正することができる

注意

医療情報システムによってはセキュリティ・パッチを適用できない場合もある

09. OSのセキュリティ・パッチ適用（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.10

1 【調査】セキュリティ・パッチ適用の可否を確認

- 現在のパソコンのOSのバージョンを確認する
- 医療情報システムが動作保証しているOSのバージョンを確認する
- セキュリティ・パッチを適用しても問題がないことを、医療情報システムベンダ等に確認する

Point

OSのサポート期限が切れている場合は、セキュリティ・パッチが適用できないため、OSのバージョンアップを計画する

2 【対策】セキュリティパッチ適用を計画する

動作保証されていない場合は、次期システム更改等により適用を計画する

- セキュリティ・パッチの適用ができる場合は、一部の端末で適用して動作検証をしたうえで、順次適用を開始する

Point

複数台のパソコン等が一度にセキュリティ・パッチを適用すると、通信量が多くなることで、システムへのアクセスが遅くなる等、業務に影響及ぼすおそれがあるため、計画的に実施する

3 【強化】セキュリティパッチの適用状況を一元管理する

Level Up!

パソコン等の台数が多い場合は、WSUSサーバ等を導入して、OSのセキュリティパッチの更新を一元管理する。

09. OSのセキュリティ・パッチ適用（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.10

Start!

OSのバージョンを確認しよう！

- Windows XP、Vista、7、8.1は既にサポートが終了しているため、機器更改する場合は、Windows10または11にする
- Windows10以降は、バージョン毎のサポート期限が定められているため、Windows10または11においても、サポート期限が切れるおそれがあることに注意する

OS	バージョン	サポート期限
Windows11	22H2	2024年10月8日
	21H2	2023年10月10日
Windows10	22H2	2024年5月14日
	21H2	2023年6月13日
	21H1以前	**サポート終了済み**

バージョンの確認方法（Windows10の場合）

① スタートを開いて「winver」と入力する

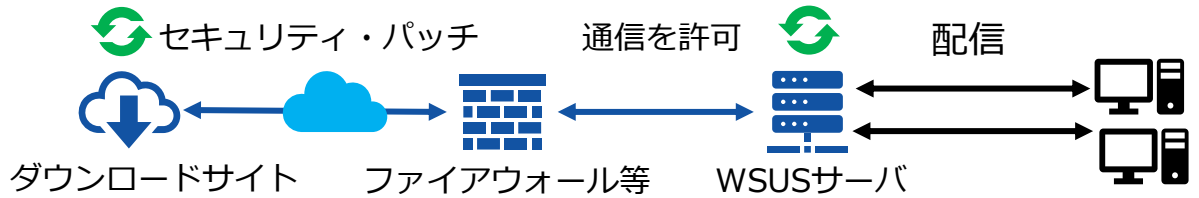
② 「Winver　コマンドの実行」をクリックすると、「Windowsのバージョン情報」画面が開くため、バージョンを確認する

※1509～2004、20H2、21H1は終了済

Level Up!

セキュリティ・パッチの適用ができる環境を準備する

- 端末とセキュリティ・パッチのダウンロードサイトの通信を許可する
- 端末台数が多い場合は、WSUSサーバを準備して、WSUSサーバから配信する



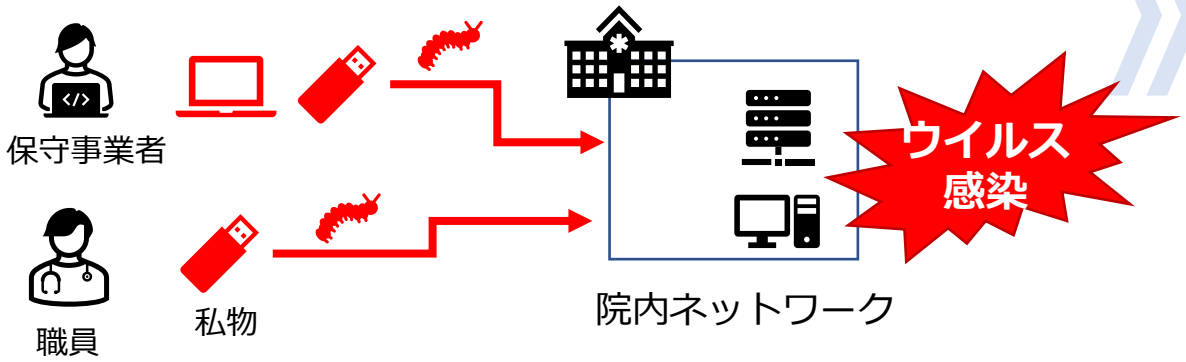
10.情報機器・記録媒体の持ち込み管理（1/3）概要

関連チェックリスト No.12、15

ウイルスが混入した情報機器（ノートパソコン、スマートフォン等）や記録媒体（USBメモリ等）を院内ネットワークに接続すると、ウイルスが拡散されるおそれがあるため、持ち込みの管理が推奨される。

想定されるリスク

- ✓ 院内ネットワークに接続する情報機器、記録媒体にウイルスが混入している
- ✓ 事前にウイルスチェックを実施しないまま、院内ネットワークに接続する

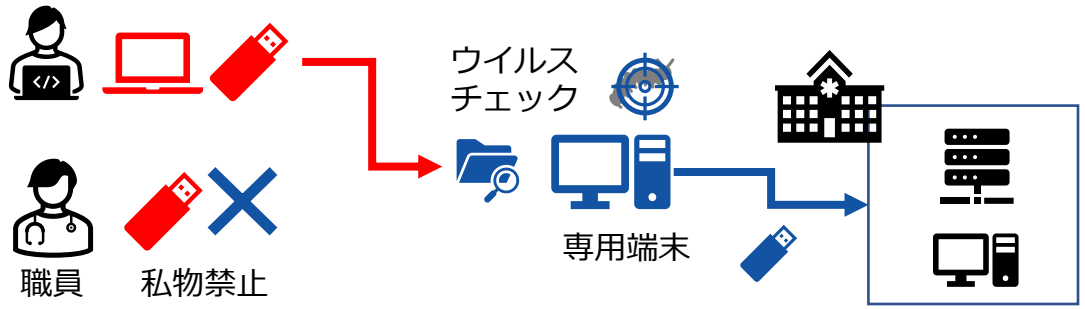


被害

持ち込まれた情報機器等を経由して、院内のネットワークにウイルスが拡散される

対策案

- ✓ 私物USBメモリ等の許可されていない情報機器等の使用しないように周知するもしくは制限する
- ✓ 外部からの情報受領時には、ウイルスが混入していないかチェックする



効果

情報機器の持ち込みによるウイルス感染を抑制できる

注意

規模が大きい場合は、接続できる機器等を制限する仕組みを検討する

10.情報機器・記録媒体の持ち込み管理（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.12、15

1 【準備】私物の情報機器・外部媒体を院内ネットワークに接続しないように注意喚起

- 私物の情報機器・記録媒体等について、院内ネットワークへの接続は原則禁止にする
  - ➢ 緊急時などを含めて私物の情報機器・外部記録媒体の接続が必要な場合は、情報システム管理者の許可を得る
- データの受渡等のために業務でUSBメモリ等の記録媒体が必要な場合は、組織内で専用のUSBメモリを準備する

Point

業務用のパソコンにスマートフォンを接続した場合、自動でデータ同期する等、予期せぬ動作を起こす可能性や、個人によるデータ持ち出しが可能になるため、**充電目的などであっても、スマートフォンの接続は禁止する**

2 【対策】持ち込まれる情報機器・記録媒体をウイルスチェックする

- 保守作業等により、院内に持ち込まれる情報機器・記録媒体を確認し、ウイルスチェック用の端末でチェックしてから接続する
  - ➢ 院内でのウイルスチェックが困難な場合は、持ち込みを行う業者にて事前にチェックするように依頼する
- 作業終了後に必要なデータ以外が持ち出されていないか確認する

Point

古いウイルスであっても、医療情報システムが、セキュリティパッチやパターンファイルを更新していない場合、感染して被害が発生するケースがある。

3 【強化】接続できる情報機器・記録媒体を技術的に制御する

Level Up!

院内ネットワークに接続できる情報機器をMACアドレス認証等により制限する。各種情報機器には資産管理ソフト等を導入して、許可されていない記録媒体等を接続できないようにする。

10.情報機器・記録媒体の持ち込み管理（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.12、15

Start!

持ち込まれた情報機器・記録媒体をチェックしよう！

- 情報機器は事前に確認し、ウイルス対策ソフトのチェック結果を確認できた機器のみ、接続を許可する
- 記録媒体はウイルス対策ソフトが導入されたウイルスチェック用の端末を用意して、以下の手順で実施する

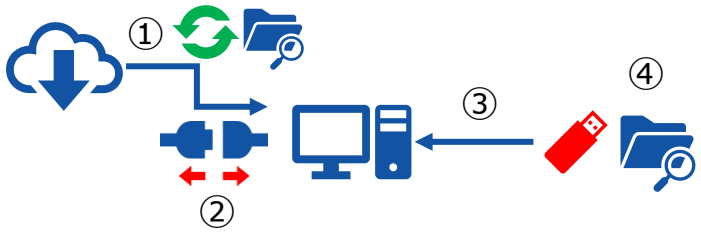
① ウイルス対策ソフトを最新のパターンファイルに更新する

② ウイルスチェック端末をネットワークから切り離す（LANケーブルを抜く等）

③ 記録媒体をウイルスチェック端末に接続する

④ ウイルス対策ソフトで記録媒体をスキャンする
- ウイルスが検出されなければ、接続を許可する
- ウイルスが検出された場合は、ウイルスチェック端末と一緒に隔離する

※ウイルスチェックにより、ウイルスが検出されなくても、ウイルスがないことを保証するものではないため注意する

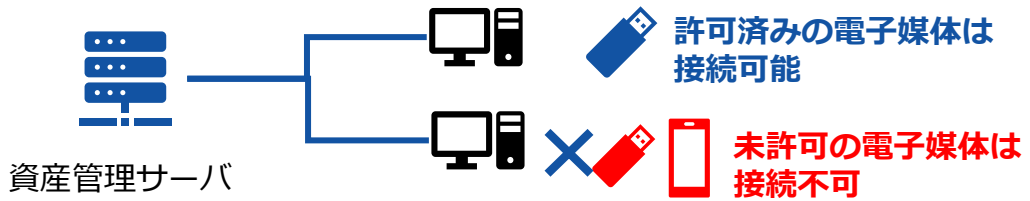


Good!

システムにより持ち込機器等の接続を制御する

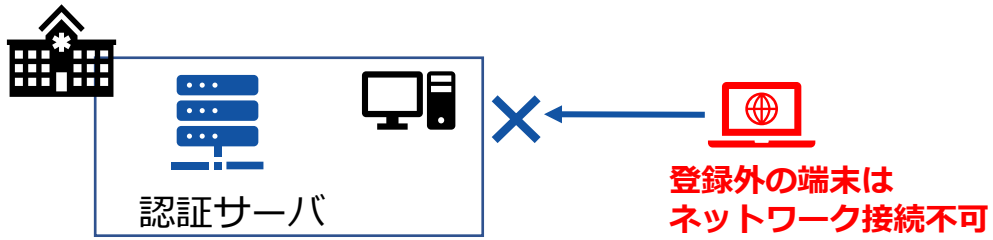
【資産管理ソフト】

登録されたUSBメモリのみ接続を許可して、操作したログを残す
※登録外の機器等の不正な接続を検知するとアラートの発信も可能



【MACアドレス認証】

MACアドレス（情報機器固有のネットワーク通信の番号）を登録した機器以外は接続できない仕組み



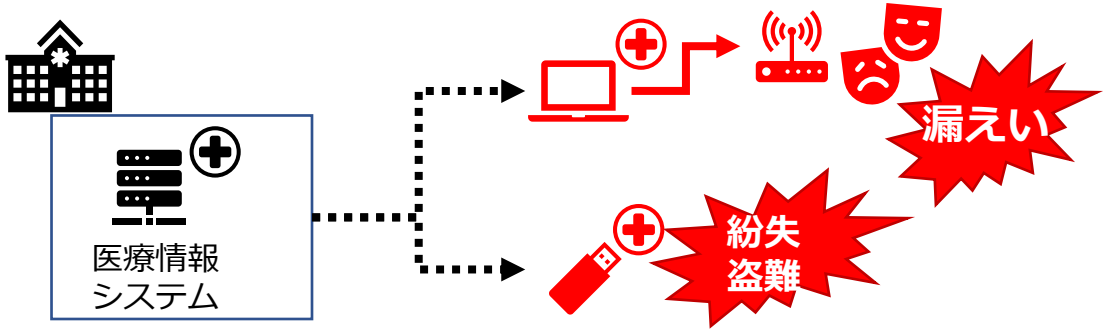
11.情報機器・記録媒体の持ち出し管理（1/3）概要

関連チェックリスト No.14

情報機器・記録媒体をセキュリティ対策が十分でない院外のネットワークに接続すると、保存している情報の漏えいやウイルス感染する恐れがあるため、外部への持ち出し管理が推奨される。

想定されるリスク

- ✓ 自宅などの対策が不十分な環境に持ち出して利用して、ウイルス感染する
- ✓ 情報機器・記録媒体に重要なデータが保存されたまま紛失する



被害

持ち出し先でサイバー攻撃を受けると対策ができない

被害

対策が十分でない環境に医療情報が保存され、漏えいしてしまう

対策案

- ✓ 持ち出す情報機器・記録媒体の利用を制限する
- ✓ 持ち出し記録を作成する
- ✓ 持出し用の情報機器・記録媒体に保存するデータは必要最小限にする

効果

機器の持ち出しによる被害を最小限にできる

注意

持ち出した機器等が他の人に利用されないように、暗号化機能などを活用する

11.情報機器・記録媒体の持ち出し管理（2/3）対策プラン

関連チェックリスト No.14

1 【準備】情報機器・記録媒体等の外部利用は業務上必要な場合に限定する

- 外部に情報機器・記録媒体等を持ち出す場合は、業務において利用が必要な場合のみとする
- 外部に持ち出すデータは業務利用に限定する
  - ➢ 自宅のパソコンや個人利用のクラウドサービス等にデータを持ち出したデータを保存しない
- 持ち出す情報機器・記録媒体の外部利用を制限する

Point

情報機器や記録媒体を持ち出した際に紛失する事故が多発している。また、外部で情報機器を利用する場合は、盗難、画面の覗き見、攻撃者が設置したフリーWi-Fiに接続することによる通信の盗聴等、持ち出した機器等を狙った攻撃にも注意が必要である。

2 【対策】持ち出しの記録を作成する

- 記録簿等によって持ち出した情報機器、記録媒体を管理する
  - ➢ 持ち出した日時、利用者、機器、利用の用途、返却時の記録を作成する
  - ➢ 長期持出の場合は、利用者に対して定期的に所在を確認する
- 返却時は不要なデータは削除する

Point

持ち出したデータが保存されたまま機器等を返却すると、次の利用者が必要以上のデータが持ち出してしまい、紛失時の影響が大きくなるおそれがある。

3 【強化】暗号化機能を有効にした持ち出し専用の情報機器・記録媒体を準備する

Level Up!

持ち出し専用に暗号化機能を有効にした情報機器や記録媒体を準備する。利用時にはパスワード入力が必要な設定にする。

11.情報機器・記録媒体の持ち出し管理（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.14

Start!

持ち出した情報機器・記録媒体の取扱いを見直してみましょう！

場面	リスク	必要な対策	備考
持出前	機器等の所在が不明になる	・持出記録の作成・申請・承認 ・機器等の施錠保管	長期間持ち出しが必要な場合は、定期的に所在を確認する 申請がなく持ち出せないようにする
	大量のデータの持ち出し	・暗号化設定・パスワード設定 ・持ち出すデータを最小限にする　等	暗号化機能付きのUSBメモリ等を準備する パソコンはBitLockerを有効にする
移動中	紛失	・かばんに入れる ・落下防止のストラップをつける　等	重要な情報を持ち出したまま、飲食店などに立ち寄り、紛失する事例が発生している
	盗難	・車内・公共交通機関にかばんを放置しない ・移動中は常に携帯する　等	車上荒らしにあうことに注意する 公共交通機関では棚の上などに放置しない
利用中	通信の盗聴	・フリーWi-Fi等の利用禁止 ・暗号化通信の利用	業務でインターネット通信が必要な場合は、モバイルWi-Fi、スマートフォンのテザリングなどを用意する
	ウイルス感染	・私物USBメモリ等の接続禁止	資産管理ソフトなどを導入して接続を制限してもよい
	覗き見の防止	・スクリーンセーバ設定 ・覗き見防止フィルタの設置	離籍時は他の人に操作されないように、画面ロックしてログインパスワード画面に戻る（「Windows」キー＋「L」キー）
	重要な情報を誤って公開する	・個人クラウドサービス・SNSの利用禁止 ・利用者以外に使用させない	個人契約のクラウドサービス等は誤って情報を公開する、乗っ取り被害にあうおそれがあるため利用させない
返却時	返却忘れ（所在が不明になる）	・返却記録の作成・申請・承認	前の利用者がデータを削除していない場合、次の利用者はデータの保存が必要か前の利用者に確認して、削除する
	次の利用者による漏えい	・不要なデータの削除	
紛失	紛失の連絡をしない	・緊急時の連絡先の周知	紛失時は連絡が遅くなると影響が大きくなるため、発覚した際は速やかに連絡し、独自の判断で対応しないように教育する

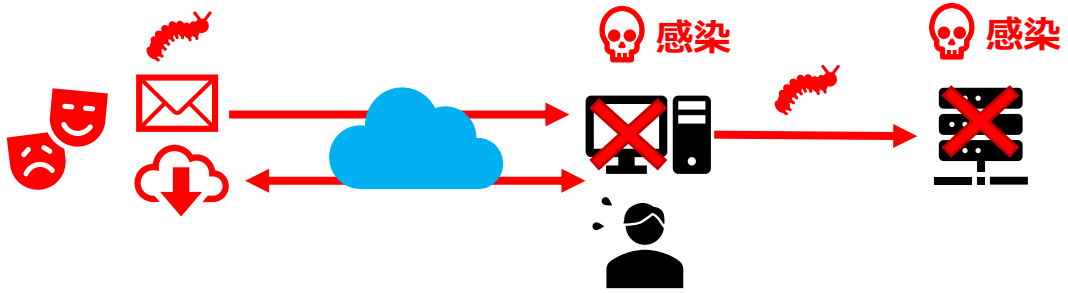
12.インターネット・電子メールの取り扱いの注意（1/3）概要

関連チェックリスト No.16、17、18

インターネット閲覧や電子メールを経由したウイルス感染について、職員に注意喚起する、またはシステムにより制限することが推奨される。

想定されるリスク

- ✓ 職員が攻撃メールに添付されたファイルや本文に記載されたリンクに気づかず開いてしまう
- ✓ 攻撃者が用意した不正なウェブサイトにアクセスして、ウイルス感染する

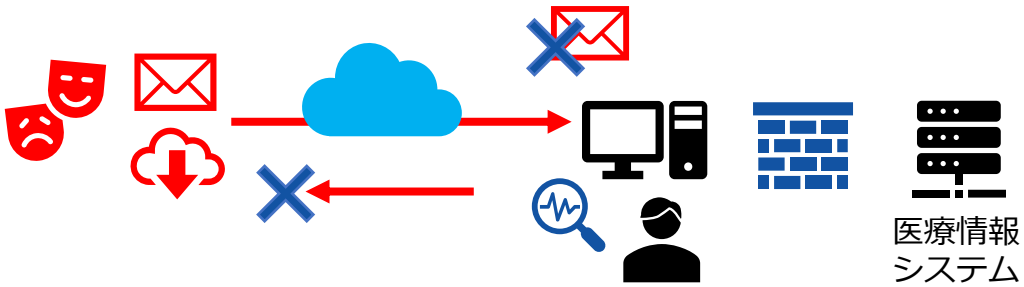


被害 攻撃メールを起点に院内ネットワークに侵入される

被害 盗み出された情報が取引先などへの攻撃に悪用され、二次被害が発生する

対策案

- ✓ 不審なメールは添付ファイルやURLをクリックせず、削除するように教育する
- ✓ 医療情報システムの利用端末からはウェブサイトを閲覧できない／閲覧できるウェブサイトを制限する



効果 インターネットを経由したウイルス感染等の被害が抑制できる

注意 ウェブサイトを閲覧するだけでウイルス感染する場合もあるので注意する

12.インターネット・電子メールの取り扱いの注意（2/3）対策プラン

関連ﾁｪｯｸﾘｽﾄ No.16、17、18

1 【調査】業務におけるインターネットの利用状況を把握する

- 業務におけるメールの利用を確認する
  - 添付ファイルはどのように取り扱っているか
  - 不審なメールが届いていないか
  - メールで重要な情報を送る場合は、パスワードを設定しているか

- 業務でのインターネット利用状況を確認する
  - 業務上必要なウェブサイトの確認
  - クラウドサービス・外部サービスの利用があるか
  - パスワードの設定（付箋に書いてモニタに貼っていないか等）

2 【対策】職員にインターネット・電子メールの取扱いに関する注意喚起をする

- **「サイバーセキュリティ対策5ヶ条」などを配布して、職員に取扱いに関する注意喚起を行う**
  - 不審なメールを発見した時は速やかに削除し、転送しないようにする
  - 不審なメールを開封した場合は、LANケーブルを抜いて隔離し、速やかにシステム管理者に報告させる（証拠保全のため端末の電源は切らない）
  - 外部にデータを送る場合は、添付ファイルにパスワードを設定し、別手段でパスワードを連絡させる
  - 業務に関係のないウェブサイトの利用を禁止する

3 【強化】インターネット・電子メールの取扱いを制限する仕組みを導入する

Level Up!

医療情報システムが接続するネットワークと電子メールを利用できる環境は分離する。不審なメールのフィルタリング設定を行う。
メールを送信する場合は、宛先のチェックなど誤送信を防止するシステムを導入する。
不審なウェブサイトへのアクセス制限やインターネットとセキュアな通信を行うシステム（VDI等）を導入する。

12.インターネット・電子メールの取り扱いの注意（3/3）具体的な対策

関連ﾁｪｯｸﾘｽﾄ No.16、17、18

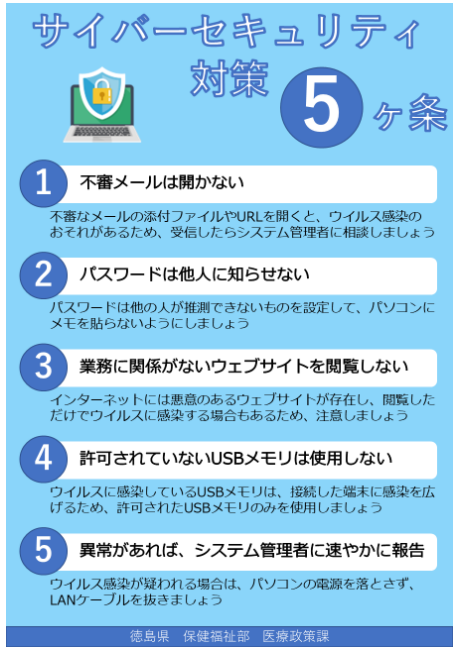
Start!

現場の職員にサイバーセキュリティに関する注意喚起をしましょう！

Check!

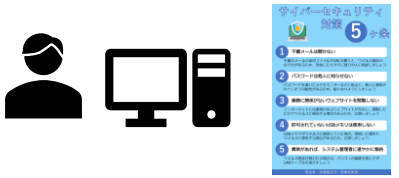
付録４：「サイバーセキュリティ対策5ヶ条」

- サイバーセキュリティ対策として職員に最低限実施してもらいたい5つの事項をまとめている
- インシデントが発生した場合に備えて、システム管理者の連絡先を周知しておく
  - ➢ システム管理者が不在時の処理も決めておくとよい



【利用イメージ】

パソコンの近くに掲示



朝礼等で配布

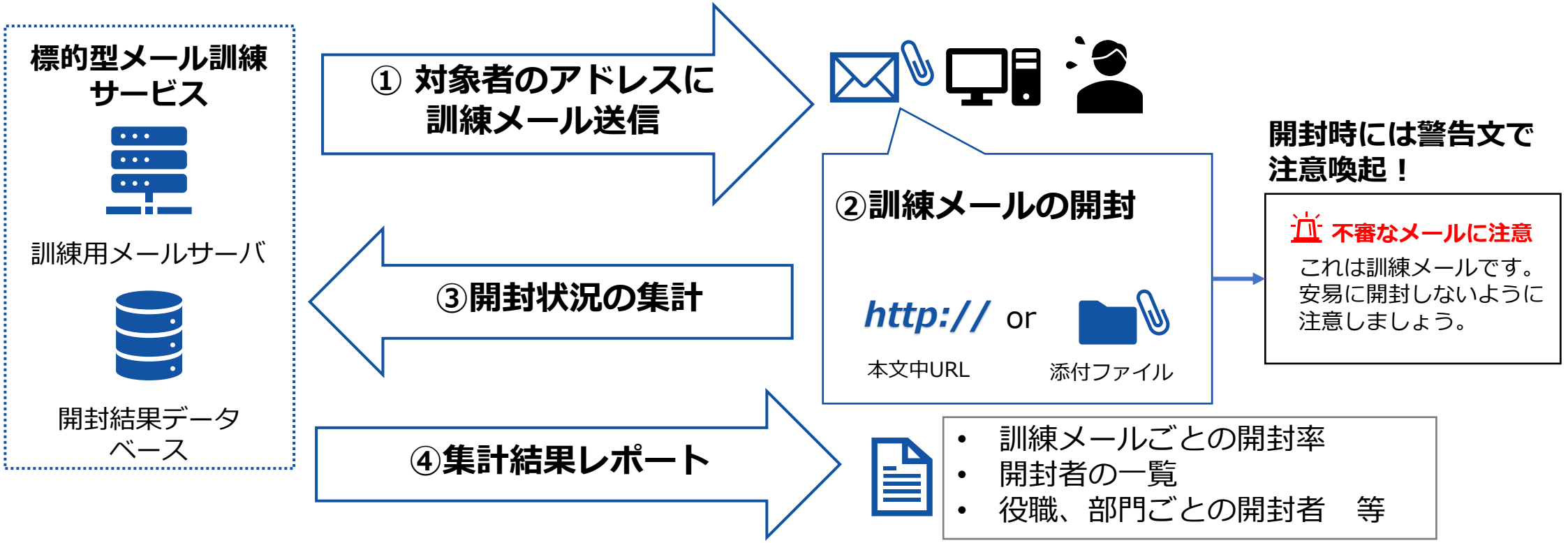
【参考】標的型メール訓練の活用

関連チェックリスト No.17

Level Up!

標的型メール訓練による実践的な対応訓練

- ウイルス感染を狙った標的型メールを模した訓練メールを、実際に組織内に送付して、添付ファイルやURLを開いた結果を集計する訓練サービスがある
- 開封時には、開封者向けの教育コンテンツによる注意喚起を行うことができる
- 実際にメールが届くため、職員の意識が向上される

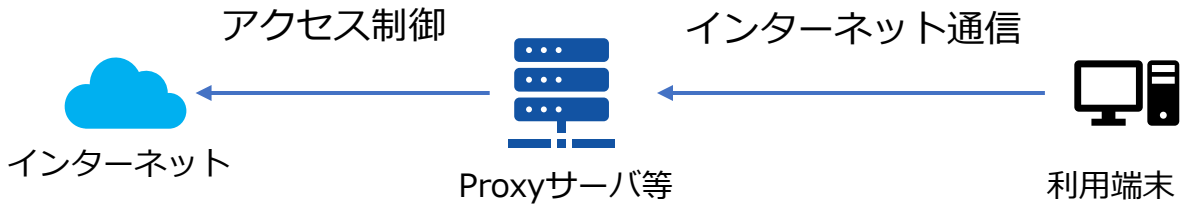


【参考】インターネット利用のセキュリティ対策

関連ﾁｪｯｸﾘｽﾄ No.16、17、18

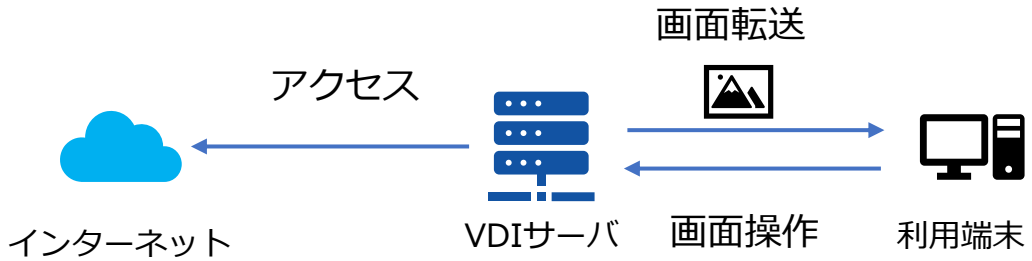
Level Up! Webフィルタリングの導入

- 不審なサイトや不正な通信をブロックする
  - 利用者は意識せずに不審なサイト等へのアクセスが制限される



Level Up! VDI（仮想デスクトップ）の導入

- VDIサーバ上に仮想デスクトップを作成し、利用端末に画面転送する。利用端末からは仮想デスクトップをリモートで操作する
  - 利用端末にはデータが残らないため、より安全にインターネット利用ができる



付録

付録

- 付録１：ネットワーク簡易構成図

  ※ 別途、医療情報システムベンダ等が作成した構成図があればご活用ください

- 付録２：サイバーセキュリティ体制図

- 付録３：外部連絡先一覧

- 付録４：サイバーセキュリティ対策５ヶ条

  ※ 各現場に回覧、掲示などして、ご活用ください。