ご質問	回答
５回のログインミスでアカウントロック１５分は、一般ユーザー権限での推奨設定でしょうか？それとも管理者権限での推奨設定でしょうか？	どのアカウントが攻撃に使われるのはかわかりませんので基本的には利用されるアカウント全てでの対応を推奨いたします。
ADによる管理の具体例を知りたい：パソコン以外の有形無形の管理ができる？	ディレクトリサービス、インベントリ管理、構成管理などの仕組みをつかって、端末だけではなく、IDやソフトウェアなど把握し、脆弱性がないかどうかある場合にはUpdateを行うなどの対応を行われているケースが多く、その多くの仕組みをクラウドサービスで実現されている企業・医療機関もあります。
ID管理において、メールひとつひとつにもIDを振るというお話がありました。また、当院には莫大な数のファイルがあるのですが、それらひとつひとつにもIDを振る必要があると思います。そのためにどのような方法があるのでしょうか。	一般的には自動的にIDが振られてメールは個別管理されていますが、そうではないケースもあります。またメールやファイルなどを複数のシステムで管理されている場合、アクセス履歴や権限管理などが個別で管理されるため可能な限り同一プラットフォームで管理する方が運用負荷は減ると考えます。最近ではそれらをクラウドサービスで利用する医療機関も増えており、ログ監視やファイルの共有状況を可視化、機密情報が含まれるデータがどこに置かれているのかなどを一元的に確認できる仕組みもございます。
ＩＴ資産管理の重要性は分かりますが、その資産を管理するシステムについてご教授いただければ幸いです。	Configuration Managerという資産管理と構成管理などを行うシステムががあります。またインターネットに接続できるPC・タブレット・スマートフォンなどはIntuneというクラウドサービスがあり、両方を利用して共同管理する事によって院内の全ての端末を一元管理することが可能です。
アカウント制御やログ管理について 電子カルテシステムや部門システムでは、行っていますがファイル共有サーバーでは行えません。 アカウントは管理者と標準アカウントの２つしかなく、管理者アカウントはシステム担当者のみログインできます。標準アカウントではデータの編集・閲覧ができますが、データをクライアント端末から抜くことは禁止されています。 データの閲覧・編集は共有情報のため、医師・看護師・リハスタッフ・医事課スタッフ等医療に関わるものが電子カルテでファイル連携で見られるようにしてあります。 また、全ての端末にウイルス対策ソフトを導入しております。 これをアカウント制御を行うようにするのは、不可能のように思いますが、どうしたらよいのでしょうか？	アカウントの共有利用は誰が実際に利用したのか、それが攻撃者なのかも把握することができない為、基本的には利用者個別にIDを付与することを推奨します。
クローズド環境とオープン環境が社内ネットであり、区分しているが、共通の資産管理ソフトがない？	クローズド・オープンのNW分離をせずに一元管理されているケースもあります。現時点でその対応が難しい場合であったとしても、共通の資産管理システムでなく、別々のものでも構いませんのでまずは院内の全ての資産を管理する事が重要だと考えます。
サーバーと端末の違いがわからなくなる時があった。ビルトインアドミニストレーターの話はサーバーの話題ですか。	全てのデバイスが攻撃される可能性がある事を前提に考えると基本的には利用されるデバイス全てでの対応を推奨いたします。
実現できている医療機関や一般企業は具体的にどのように実現されているのでしょうか？	ディレクトリサービス、インベントリ管理、構成管理などの仕組みをつかって、端末だけではなく、IDやソフトウェアなど把握し、脆弱性がないかどうかある場合にはUpdateを行うなどの対応を行われているケースが多く、その多くの仕組みをクラウドサービスで実現されている企業・医療機関もあります。
他施設で取り組んでいるセキュリティ対策情報があれば是非紹介して頂きたいです	ディレクトリサービス、インベントリ管理、構成管理などの仕組みをつかって、端末だけではなく、IDやソフトウェアなど把握し、脆弱性がないかどうかある場合にはUpdateを行うなどの対応を行われているケースが多く、その多くの仕組みをクラウドサービスで実現されている企業・医療機関もあります。