4. 技術的・物理的対応

チェックリスト項目	説明	対策例	関連資料
(1)ネットワーク	【狙い】 大学において様々な用途でサーバ・クライアントが利用され、守るべき情報の多くはネットワーク上でやり取りされています。 SaaS(Software as a Service)や、それを内包するクラウドコンピューティングなど学外のサービスを利用する場合においても、情報の流れとその制御には注意する必要があります。 この部分では、情報の流れをコントロールするために必要なネットワークに対するチェックを狙いとしています。		
・ファイアウォールを導入し、ポリシーに基づきログ管理や通信の状況を定期的に点検しているか。	今日のインターネットは、不正侵入・ウィルス(ワーム)の感染、違法なファイル共有等、悪意のあるネットワーク利用の存在を無視できません。したがって、学内LANをインターネットに接続する場合、このようなネットワーク利用から大学の情報資産や利用者を守るために、また大学が他組織に対するネットワーク攻撃等に加担しないように、ファイアウォール等による学内LANの保護が必要です。 ファイアウォールは、性能や対応するネットワークインターフェースにより価格の幅が広く、また最近では、ファイアウォールの機能だけでなく、不正侵入検知・防御システム(IDS/IPS)の機能を有するものや、ウイルス対策機能、Webコンテンツフィルタリング等の機能を併せ持った統合脅威管理(UTM)アプライアンス等もあります。 ファイアウォールの導入に際しては、どのような設定を施すのか、インターネット利用の利便性とネットワークセキュリティの確保のバランスを考慮して、十分に検討しなければなりません。 また、導入後の運用においても、新たなネットワークアプリケーションの登場や未知のネットワークセキュリティ上の脅威に備えて、定期的にログや通信状況を点検することが重要です。	・ファイアウォール(またはそれに準拠する機器)の導入 ・通信の制御ポリシー(ファイアウォールの設定)の策定 ・学外・学内・DMZでの通信ルールの明確化 ・ファイアウォールに関する現状把握 ・ネットワーク運用方法(機器の保守・監視・運用管理体制・アウトソーシング)の見直し ・ファイアウォールの定期的な点検の体制・ルール作り	平成18年度大学情報セキュリティ研究講習会資料 B-1 ネットワーク基本技術コース ・第五部インターネットセキュリティ「5.2.1ファイアウォール」 平成18年度大学情報セキュリティ研究講習会 A-2 情報管理コース ・東京理科大学におけるセキュリティ技術の取り組みについて「2-3.キャンパス内ネットワーク/2-4.FWの運用方針」
・不正侵入検知・防御システムを導入し、検知対象の情報を日々更新し、ログの保存・解析を行っているか。	インターネットの利用のために、ファイアウォールでは遮断できない(許可せざるを得ない)通信については、不正侵入検知・防御システムによる学内LANの保護が有効です。不正侵入検知・防御システムは、シグネチャと呼ばれる特徴的な通信パターンの定義情報を基にネットワークの監視を行うため、定義情報の更新は運用上重要です。 なお、ファイアウォールによる学内LANの保護が十分に機能すると判断されれば、不正侵入検知・防御システムを導入しないという選択もありえます。	・不正侵入検知・防御システム(IDS/IPS)の導入 ・検知・防御の制御ポリシーやシグネチャ更新のポリシー(IDS/IPSの設定)の設定 ・定期的な点検の体制・ルール作り ・ネットワーク運用方法(機器の保守・監視・運用管理体制・アウトソーシング)の見直し	平成18年度大学情報セキュリティ研究講習会 B-1 ネットワーク基本技術コース ・第五部インターネットセキュリティ「5.2.2IDS/5.2.3IPS」
・組織が管理するネットワークを把握し、トラフィック監視を行っているか。	学内LANは、ネットワークインフラとして、学内の隅々に整備されていると思われます。そして、学内LANは電子メールや共有ファイル等情報資産そのものの通り道です。したがって、基幹部分から情報コンセントに至るまで、学内全ての構成を把握しておく必要があります。 また、トラフィックの監視は、平常時の利用状況の把握や可用性確保のために重要です。ネットワークを流通するコンテンツは増加傾向にあるため、将来的な整備計画の立案のためにも、欠かすことができません。	・ネットワーク構成図の作成 ・情報コンセント設置場所の把握 ・ネットワーク管理体制の整備(責任の所在の確認) ・トラフィック監視システムの導入(監視箇所の選定) ・平常時のネットワークトラフィックの把握 ・将来的なネットワーク整備計画の立案	平成19年度大学情報セキュリティ研究講習会 C.ネットワーク運用管理コース 1.サーバ・ネットワークのモニタリング
・業務・研究・教育など用途ごとにネットワークを分離しているか。	学内のネットワークの用途を大きく分類すると、業務・研究・教育に分けられますが、それぞれの用途では扱う情報の種類や利用特性が異なります。それぞれが物理的または論理的に分離されたネットワーク構成であれば、運用ポリシーやガイドライン等の作成の際、用途別に明確な対策を検討することが容易になります。 諸事情により分離されていない、また分離が難しい場合には、ネットワークを利用して扱う情報の重要度に応じて、通信経路の暗号化(SSL通信やVPN)等を検討しましょう。	・用途ごとのネットワークの構築 ・情報の重要度に応じた通信経路の確保 ・情報の重要度に応じた通信の暗号化	平成18年度大学情報セキュリティ研究講習会 A-2 情報管理コース ・東京理科大学におけるセキュリティ技術の取り組みについて「2-3.キャンパス内ネットワーク/2-4.FWの運用方針」 ・情報漏洩・不正侵入防止などセキュリティ技術の動向確認と対応策の検討「対策の考え方:ゾーニング」
・セキュリティ対策のなされていない無線LANのアクセスポイントはないか。	無線LANは、ケーブル接続が不要であるという利便性の高さから広く利用されています。しかし、電波の届く範囲にある端末は通信可能という無線LANの特徴が、時にセキュリティの弱い部分になる場合があります。したがって、無線LANのアクセスポイントを設置する際には、利用が許可される人または端末以外の通信を遮断するように、なんらかの対策が必要です。更に、無線LANによるネットワークは電波による通信であるため、悪意のある者によって通信が傍受されてしまう可能性があることを常に心掛ける必要があります。	・無線LANによるネットワーク構築のルール作り ・無線LANによるネットワークの安全性の調査	平成18年度大学情報セキュリティ研究講習会 B-1 ネットワーク基本技術コース ・第五部インターネットセキュリティ「5.2.5無線LAN」 B-2 ネットワーク運用管理コース ・無線LANのセキュリティ
・ユーザ認証なしでだれでも利用できる情報コンセント等はないか。	学内におけるネットワークの利用は、コンピュータ実習室や研究室だけでなく、一般教室や会議室等に広がっています。また、学外者でも立ち入り可能な場所が多いという大学特有の事情もあります。大学の情報資産であるネットワークが適切に利用されるように、情報コンセントの利用については、何らかの技術的・物理的な対策が必要です。	・情報コンセントの設置場所の把握 ・情報コンセントの利用に関するルール作り ・情報コンセントを鍵付きの扉に収納 ・情報コンセントのある部屋を施錠	平成18年度大学情報セキュリティ研究講習会 A-2 情報管理コース ・中部大学の教育用ネットワークのセキュリティと認証 ・東京理科大学におけるセキュリティ技術の取り組みについて「2-5.情報コンセント」
・ルータやスイッチなどのアクセスコントロールや時刻同期を行っているか。	学外との接続にファイアウォールを設置している場合でも、学内の基幹ネットワーク等の要所において、不要な通信や不適切な通信を遮断するためにアクセスコントロールを行うことは、ネットワーク帯域の適切な利用のために有効です。 インテリジェントなネットワーク機器は、インターフェースやポートのリンクの状態をログに出力する機能を持っています。これらのネットワーク機器の時刻同期を適切に行っておくことで、ネットワークトラブルの発生時の調査や復旧の重要な情報になります。	・不要な通信や不適切な通信の洗い出し ・アクセスコントロールの設定 ・NTPサーバの構築 ・ネットワーク機器の時刻の同期 ・ネットワーク機器のログ採取の設定	平成18年度大学情報セキュリティ研究講習会 B-1 ネットワーク基本技術コース ・第二部ネットワークシステム基礎「ルータ/ルータと経路情報/ルーティングテーブル」 平成21年度大学情報セキュリティ研究講習会 A.情報セキュリティインシデント対応コース 1.監視システムの整備「NTPの設定」

チェックリスト項目	説明	対策例	関連資料
(2)サーバ	【狙い】 大学において扱われる情報の多くは、サーバ上に保存されています。また、それらの情報は、サービスとして様々な形態で、クライアントを通して利用者に提供されています。 メンテナンス性や耐障害性などからサーバをデータセンターに設置する場合においても、大学に関連するサービスを提供する機器であれば、情報セキュリティ対策の適用範囲に含まれます。 この部分では、守るべき情報を適切に管理するために必要なサーバに対するチェックを狙いとしています。		
・OSやサーバのソフトウェアは信頼できるバージョンを使用し、必要に応じてアップデートを行っているか。	OSやソフトウェアの脆弱性は日々報告され、メーカーもこれをアップデートする方法を提供しています。また、OSやソフトウェアに対する脅威は、既知の脆弱性を利用しているものが多いため、最新バージョンへアップデートすることは、最低限の対策といえます。なお、なんらかの制約により最新バージョンの利用ができない場合においても、そのリスクを認識し対策を施す必要があります。 現状、全てのOSやソフトウェアの脆弱性の一つひとつについて、その影響を調査・検討してアップデートを適用することは現実的でないので、自動アップデート機能等が有効活用されています。しかし、自動アップデート後にサービスに対する想定外の影響が発覚することに備えて、アップデート以前の状態まで復旧できるようバックアップを採取しておく等、慎重に行う必要があります。	・サーバ構成の把握(OSとバージョン・稼働サービス) ・アップデート方法の確認(自動・手動) ・アップデート作業手順の整備 ・定期的なアップデート確認の体制・ルール作り ・サーバの運用方法(機器の保守・監視・運用管理体制・アウトソーシング)の見直し	総務省「国民のための情報セキュリティサイト」 ・自設サーバー利用者のための情報セキュリティ対策-実践編「ソフトウェアの更新」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_homepage/server02.htm
・サーバの稼動状況や利用者ごとのアクセス状況を把握し、正確な時刻設定のもと、ログの保存と解析を行っているか。	サーバの稼働状況やアクセス状況の監視は、平常時の利用状況の把握や適切なサーバ資源の配分等、可用性確保のために重要です。これらの情報は、将来的なサービスの増強またはサービスの廃止等の判断資料としても有効です。 また、時刻同期を行った上でログを保存することは、サーバ運用において最重要事項です。ログは、サーバトラブルやインシデントの発生時に重要な情報となります。	・サーバ構成図(サービス構成図)の作成 ・サーバ管理体制の整備(責任の所在の確認) ・サーバ監視装置(システム)の導入(監視項目の選定) ・NTPサーバの導入 ・サーバの時刻同期 ・各種ログの適切な保存設定 ・平常時のサーバ負荷の把握 ・将来的なサービスの増強・廃止計画の立案	平成21年度大学情報セキュリティ研究講習会 A.情報セキュリティｲﾝｼﾃﾞﾝﾄ対応コース 1.監視システムの整備 平成19年度大学情報セキュリティ研究講習会 C.ネットワーク運用管理コース 1.サーバ・ネットワークのモニタリング
・不要なサービスやポート、アカウント等が稼動していないか。	サーバとして運用するサービスについては、注意を払って設定や運用状況の把握がされますが、OSが標準で実行しているサービスについても注意が必要です。このようなサービスが、気付かないセキュリティホールにならないよう、運用に不要なサービスは予め停止しておき、必要以上のポートにアクセスできないようにする必要があります。 また、サーバの管理アカウントについても、不必要に多く登録したり、必要以上の権限を与えたりしないよう、パスワードの取り扱いも含めて注意する必要があります。	・不要なサービスの停止 ・ポートスキャンによるサーバのセキュリティ監査 ・必要最低限の管理アカウントの登録 ・不要な管理アカウントの削除 ・適切なパスワードの取り扱いのルール作り	平成18年度大学情報セキュリティ研究講習会 B-1 ネットワーク基本技術コース ・第四部ネットワークアプリケーション 総務省「国民のための情報セキュリティサイト」 ・自設サーバー利用者のための情報セキュリティ対策「サーバー設定の確認」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/homepage/server04.htm
・定期的な監査を行い、セキュリティの基準を満たしていないサーバがないかチェックしているか	セキュリティに関しては新たな脅威が次々と発生し、OSやソフトウェアの脆弱性も日々報告されています。導入時にしっかりとセキュリティ対策を取り、自動的にアップデートされるように設定していたとしても、定期的にセキュリティ対策の状況を確認することは必要です。対策の足りない点を見つけたり、新たな対策の必要性を見つけたりすることがあるでしょう。	・サーバ構成図(サービス構成図)の作成 ・サーバ管理体制の整備(責任の所在の確認) ・サーバ監視装置(システム)の導入(監視項目の選定) ・定期的なセキュリティチェックの体制・ルール作り ・専門会社によるセキュリティ診断サービスの利用	総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策-実践編「セキュリティ診断」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin02.htm
・セキュリティホールとなるようなソフトウェアへの対策を行っているか。	OSやソフトウェアを問わず、セキュリティホールとなり得る部分が残存する場合は、代替の対策を慎重に検討しなければなりません。 運用上必要になるソフトウェアが未対応のためOSを最新バージョンできない場合やセキュリティ上の問題が発覚したソフトウェアにもかかわらず最新版にアップデートできない場合等でも、顕在化するリスクを検討して、リスクを最適化するように対策を施す必要があります。 ただし、このようなセキュリティホールが残るサービスやシステムについての対策を継続することは、リスクの残存だけでなく運用コストもかかるため、サービスやシステムの構築時になるべく排除できるように検討する必要があります。	・セキュリティホールが残存するサービス・システムの洗い出し ・セキュリティホールに関する情報の入手 ・代替対策の検討(リスクの評価と対応)	総務省「国民のための情報セキュリティサイト」 ・自設サーバー利用者のための情報セキュリティ対策-実践編「ソフトウェアの更新」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_homepage/server02.htm
・障害発生時の復旧に備えて、バックアップをとっているか。	ハードウェアトラブルに対しては、保守契約の締結や代替機器・保守部品を備えておくことができます。また、サーバのOSやソフトウェアに対しては、再インストール等の対応が取れます。しかし、運用している間に作られた情報は、代わりになるものがないため、重要度に応じてバックアップを採取しておく必要があります。また、採取したバックアップから、完全にリストアできることを確認しておく必要もあります。バックアップは、システムが完全に壊れてしまった場合でも、ある時点の状態まで復旧できるように作成しておくことが必要です。	・サービス・システム毎のバックアップの必要性の検討 ・バックアップの採取方法の検討 ・リストア方法の検討と確認 ・バックアップの保管場所の検討	総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「情報資産のバックアップ」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin05.htm
・施錠された安全な場所に設置し、入退室者の記録をとっているか。	サーバは情報システムを構成する重要な要素であるため、機器類への物理的なアクセスを管理しなければなりません。特に、重要な情報を扱うサーバの設置場所における入退室者の記録を取ることは、管理者が不正行為に及ばないようなけん制効果やインシデント発生時の調査に有効です。	・サーバ設置要件の検討 ・入退室管理の仕組みの検討	総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「サーバー室の情報セキュリティ対策」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin08.htm
・廃棄あるいは返却する際に、情報資産が流出しないよう、手順や履歴の管理を行っているか。	サーバやハードディスクには、当然のことながら、運用するサービスに関わる情報が保存されています。大学においては、学生の成績情報など個人情報や、教職員の人事情報、大学の経営に関わる会計情報等の重要な情報が保存されているサーバが存在するでしょう。 これらのサービスを構成していた機器類が廃棄される場合には、情報を適切に移行すると共に、情報が確実に消去されるよう注意を払う必要があります。特に、機器類をリースしていた場合等は、返却後に再利用される可能性があることを考慮して、重要な情報は確実に消去してから返却するようにします。	・機器類の廃棄時に確実に消去すべき情報資産の明確化 ・情報を消去する手順の確立(実作業・証明書類)	情報処理推進機構(IPA) ・情報セキュリティ：対策のしおり「情報漏えい対策のしおり ver.3」 http://www.ipa.go.jp/security/antivirus/shiori.html 総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策-実践編「コンピュータやメディアの廃棄」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin06.htm

チェックリスト項目	説明	対策例	関連資料
・パスワードを定期的に変更し、容易に推測できないものとなっているか。	サーバにアクセスする際に使用するアカウントは、取り扱いに十分注意し、同一のパスワードを長い期間使い続けることは避け、関係者以外が推測可能な文字列は決して使ってはなりません。 また、できる限り使い回しを避けて、作業を行った者を遡って調べられるようにしましょう。サーバとして運用するOSやサービスを構成するシステムの都合により、個別のアカウントが利用できない場合でも、作業可能な者を限定する等の対応を取るようにする必要があります。	・サーバ管理用アカウントの取り扱いに関するルール作り ・パスワードの取り扱いに関するルール作り	総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「適切なパスワード管理の推奨」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin07.htm
・不正侵入対策として、学外から管理者権限でサーバにログインできないようになっているか。	管理者権限は、サーバ運用上、非常に重要なアカウントであることは言うまでもありません。サーバの管理においては、学外ネットワークからのアクセスだけでなく、学内LANからアクセスする場合でも、直接管理者権限でログインできないように制限する必要があります。	・サーバへのログイン方法の確認 ・ログイン制限の設定	情報処理推進機構(IPA) ・情報セキュリティ：対策のしおり「不正アクセス対策のしおり ver.3」 http://www.ipa.go.jp/security/antivirus/shiori.html
・Webサーバ上のコンテンツに対するアクセス権などを適切に設定しているか。	Webサーバで公開しているコンテンツ(ファイルやフォルダ)は、適切にアクセス権を設定し、不注意による情報の書き換えや消失を防ぐために、許可されていないユーザによる操作は制限しましょう。 また、公開する必要のないコンテンツは、Webサーバ上に保存しないようにしましょう。なお、一旦公開され、後にその必要がなくなったコンテンツは、速やかにかつ確実に削除されるように作業を徹底します。	・アクセス権を設定するためのユーザ管理基盤の整備 ・Webサーバ上のコンテンツのアクセス権の確認 ・Webサーバ上で公開されているコンテンツの整理	情報処理推進機構(IPA) ・情報セキュリティ：脆弱性対策：安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html
・Webアプリケーションに対する脆弱性対策(XSS,SQLインジェクション等)を行っているか。	OSやソフトウェアの自動アップデート機能が普及してきたことで、近年のセキュリティホールに対する攻撃は、Webアプリケーションを対象にする傾向が高まっています。Webサーバは、サービスの性質上、様々なユーザからのアクセスを受け入れる必要がありますが、Webアプリケーションの脆弱性を抱えたまま運用することは、非常に危険です。特に、クロスサイトスクリプティング(XSS)やSQLインジェクションといった手法は広く知られているため、このような脆弱性が潜んでいないかどうか、Webアプリケーションを早急に点検し改善する必要があります。	・運用中のWebアプリケーションの把握 ・Webアプリケーションの脆弱性の点検 ・専門会社によるセキュリティ診断サービスの利用	平成20年度大学情報セキュリティ研究講習会 A.情報システム管理者コース 3.SQLインジェクション/クロスサイトスクリプティング 平成19年度大学情報セキュリティ研究講習会 C.ネットワーク運用管理コース 3.Webアプリケーションのセキュリティ 情報処理推進機構(IPA) ・情報セキュリティ：脆弱性対策：安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html
・重要な情報を取り扱う場合は暗号化を行っているか。	ユーザがサービスを利用する際のパスワードや重要な情報がやり取りされる場合には、通信経路でのパケットキャプチャ等による盗聴を防ぐために、通信を暗号化しましょう。Webサーバとの暗号化通信にはHTTPS(HTTP over SSL)が広く利用されていますが、その他のサービス(メール・ファイル転送・リモート接続等)についても、パスワードを使う場合は、パスワードの文字列が平文(plain text)としてネットワーク上を流れるような運用は避ける必要があります。	・暗号化通信を行うべきサービスの洗い出し ・暗号化通信を行うシステムの導入	平成20年度大学情報セキュリティ研究講習会 B.情報システム運用支援者コース 3.コンピュータ上の情報漏えい対策 平成19年度大学情報セキュリティ研究講習会 B.ネットワーク基本技術コース ネットワーク通信のセキュリティ
・公開している情報が本当に正しいものなのか定期的にチェックしているか。	公開している情報を悪意のある者が書き換える可能性だけではなく、関係者が不注意で情報を書き換えてしまう場合もあるので、公開している情報が正しいことの確認は、定期的に行うことが必要です。	・公開しているコンテンツの確認(ファイルやデータベースのサイズの変化・タイムスタンプ) ・改竄検知システム導入	ITmediaエンタープライズ ・第1回：Tripwireを導入する http://www.itmedia.co.jp/enterprise/0209/11/n13.html ※2002年9月の情報
・迷惑メール対策（ウイルス対策、spam対策、オープンリレー対策等）をしているか。	インターネットを流れるメールの大部分が迷惑メールと言われており、メールサーバの運用において迷惑メール対策は欠かすことができません。 受信してしまう迷惑メールの対策には、ブラックリスト方式によるブロッキングや意図的にレスポンスを低下させるスロットリング、メールの内容により判断するフィルタリング等があります。それぞれの対策の仕組みを考慮して、適切な対策を選択しましょう。また、OP25BやSMTP-AUTH等、学内から迷惑メールを送信させないための対策も検討が必要です。	・受信される迷惑メール対策の見直し・導入 ・送信される迷惑メール対策の見直し・導	平成20年度大学情報セキュリティ研究講習会 A.情報システム管理者コース 1.spam対策にまつわるトラブル/送信ドメイン認証技術 平成19年度大学情報セキュリティ研究講習会 C.ネットワーク運用管理コース 4.迷惑メール対策 IAjapan(財団法人インターネット協会) ・有害情報対策ポータルサイト―迷惑メール対策編― http://www.iajapan.org/anti_spam/portal/ 迷惑メール対策推進協議会迷惑メール相談センター ・迷惑メール対策ハンドブック2009 http://www.dekyo.or.jp/soudan/anti_spam/index.html#hb
・ネームサーバのデータベースが適切に管理されているか。	DNSはインターネットの重要な基盤であり、ネームサーバの停止やデータベースの不備は、インターネット利用の可用性を多大に失うので、十分な管理のもとに運用しなければなりません。トラブルの発生に備えて、DNSに冗長性を持たせることはもちろん、データベースの変更作業には、ミスが起こらないように作業手順を検討することが必要です。	・ネームサーバの構成の見直し ・ネームサーバの監視体制の整備 ・ネームサーバのデータベースの変更作業手順の作成	平成21年度大学情報セキュリティ研究講習会 A.情報セキュリティｲﾝｼﾃﾞﾝﾄ対応コース 4.フィッシング詐欺とDNSキャッシュポイズニング 5.DNSSEC～DNS SECurity extensions～ 平成18年度大学情報セキュリティ研究講習会 B-1 ネットワーク基本技術コース 第一部インターネットの基礎「1.6DNS(Domain Name Service)」 情報処理推進機構(IPA) ・情報セキュリティ：DNSキャッシュポイズニング対策 http://www.ipa.go.jp/security/vuln/DNS_security.html
・ファイルサーバへのアクセス権を適切に設定しているか。	ファイルサーバによるファイル共有は、アクセス権を慎重に検討し、許可された者以外が読み取りや書き込みできないようにしましょう。また、本来ファイル共有する必要のない情報は、ファイルサーバ上には保存しないようにします。	・アクセス権を設定するためのユーザ管理基盤の整備 ・ファイル共有領域のアクセス権の確認 ・ファイルサーバでファイル共有している情報の整理	総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「ユーザー権限とユーザー認証の管理」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin02.htm

チェックリスト項目	説明	対策例	関連資料
(3)クライアント	【狙い】 業務・教育・研究等で作られ、処理される情報が直接出入りするのは、利用者の手元にあるクライアントです。一般にクライアントは台数が多いため、対策に手間がかかる部分ですが、最も注意しなければならない部分です。 この部分は、情報が直接出入りする重要な機器であるクライアントに対するチェックを狙いとしています。		
・悪意のあるソフトウェア対策を行っているか。	学内において最も台数が多く、またセキュリティ上最も弱くなりがちなのが、日常的に利用されるクライアントです。ウイルスに感染したクライアントがボットネットを形成し、迷惑メール送信やDDoS攻撃等に利用されていることは広く知られており、他組織に対するネットワーク攻撃の加害者にならないためにも、クライアントには十分な対策が必要です。ただし、研究教育用や業務用のクライアントは同一仕様で展開されていることが多く、OSやソフトウェアの自動アップデート機能を利用すれば、比較的容易に対策が取れるでしょう。なお、研究室等で利用されているクライアントに関しても、OSやソフトウェアのアップデートを行うよう、ルール・ポリシーを整備する必要があります。 また、いわゆるファイル共有ソフトについても、違法なコンテンツの流通や情報漏えいの原因となっている現状を鑑み、適切な対策を取る必要があります。	・クライアント構成の把握(台数、OSとバージョン、設置場所・用途) ・クライアントにインストールされているソフトウェア構成の把握 ・アップデート方法の確認(自動・手動) ・ 定期的なアップデート確認の体制・ルール作り ・ ウイルス対策ソフトの導入	平成20年度大学情報セキュリティ研究講習会 B.情報システム運用支援者コース 2.クライアント・サーバサービスにおけるクライアントの設定 3.コンピュータ上の情報漏えい対策 平成18年度大学情報セキュリティ研究講習会 ・P2Pファイル共有 総務省・経済産業省連携ボット対策プロジェクト ・サイバークリーンセンター https://www.ccc.go.jp/ 情報処理推進機構(IPA) ・情報セキュリティ:対策のしおり「ウイルス対策のしおり ver.6」「スパイウェア対策のしおり ver.7」「ボット対策のしおり ver.6」 http://www.ipa.go.jp/security/antivirus/shiori.html
・OSやソフトウェアは信頼できるバージョンを使用し、必要に応じてアップデートを行っているか。	OSやソフトウェアの脆弱性は日々報告されており、メーカーもこれをアップデートする方法を提供しています。また、OSやソフトウェアに対する脅威は、既知の脆弱性を利用しているものが多いため、最新バージョンへアップデートすることは、最低限の対策といえます。なお、なんらかの制約により最新バージョンの利用ができない場合においても、そのリスクを認識し対策を施す必要があります。 現状、全てのOSやソフトウェアの脆弱性の一つひとつについて、その影響を調査・検討してアップデートを適用することは現実的でないので、自動アップデート機能等が有効活用されています。しかし、自動アップデート後にソフトウェアに対する想定外の影響が発覚する可能性があることに注意が必要です。	・クライアント構成の把握(台数、OSとバージョン) ・クライアントにインストールされているソフトウェア構成の把握 ・ソフトウェアライセンスの管理体制の整備 ・アップデート方法の確認(自動・手動) ・アップデート作業手順の整備 ・定期的なアップデート確認の体制・ルール作り	情報処理推進機構(IPA) ・情報セキュリティ:対策のしおり「ウイルス対策のしおり ver.6」「スパイウェア対策のしおり ver.7」「ボット対策のしおり ver.6」「インターネット利用時の危険対策のしおり ver.1」 http://www.ipa.go.jp/security/antivirus/shiori.html
・不要なサービスやポート、アカウント等が稼動していないか。	クライアントとして利用している場合でも、OSが標準で実行しているサービスや小規模のサーバとして実行しているサービス等が気付かないセキュリティホールにならないよう、運用に不要なサービスは予め停止しておき、必要以上のポートにアクセスできないようにすることが必要です。 また、クライアントにログインするアカウントやクライアントの管理アカウントについても、不必要に多く登録したり、必要以上の権限を与えたりしないよう、パスワードの取り扱いも含めて注意が必要です。	・不要なサービスの停止 ・ポートスキャンによるクライアントのセキュリティ監査 ・必要最低限のログインアカウント・管理アカウントの登録 ・不要なログインアカウント・管理アカウントの削除 ・適切なパスワードの取り扱いのルール作り	平成21年度大学情報セキュリティ研究講習会 B.情報システム運用支援者コース 2.クライアント・サーバサービスにおけるクライアントの設定
・正確な時刻設定のもと、利用者のログの保存と解析を行っているか。	クライアントのログインログを取ることは、その端末の使用履歴を取ることになり、インシデントの発生時の重要な情報になります。また、ログインログの採取に際しては、他のサービス・システムのログと突き合わせて利用されることを考慮し、時刻同期を行っておくことが必要です。	・NTPサーバの導入 ・クライアントの時刻同期の設定 ・ログインログの適切な保存設定	平成21年度大学情報セキュリティ研究講習会 A.情報セキュリティｲﾝｼﾃﾞﾝﾄ対応コース 1.監視システムの整備 平成20年度大学情報セキュリティ研究講習会 A.情報システム管理者コース 2.不適切な掲示板投稿への対応
・障害発生時の復旧に備えて、バックアップをとっているか。	サーバと比べると重要度は高くないものの、クライアントについても重要度により情報のバックアップを採取しておく必要があります。なお、情報の消失が、業務や教育研究活動に大きく影響を及ぼす場合は、ファイルサーバと同等に適切な管理とバックアップが行われるようにしましょう。 また、可用性を重視するのであれば、情報をファイルサーバ等に保存して適切なアクセス制限の下に管理することを検討しましょう。	・クライアントに保存されている情報のバックアップ ・バックアップの採取方法の見直し ・バックアップの保管場所の見直し	総務省「国民のための情報セキュリティサイト」 ・社員・職員全般のための情報セキュリティ対策-実践編「定期的なバックアップの実行」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/work04.htm
・部外者が容易に立ち入らないような監視体制と盗難防止策を講じているか。	クライアントやハードディスク等、利用者の身の回りに重要な情報資産があることを踏まえて、部外者が許可なくクライアントを利用できたり、簡単に情報を持ち出したりできないような対策が必要です。部外者でも立ち入ることができる場所があるのは大学特有の事情といえますが、重要な情報を扱う場所への立ち入りは制限しなければなりません。その他の場所においても、無人にならないような管理体制や機器類をワイヤーで固定する等の盗難防止策を、必要に応じて実施することも必要です。	・利用者の身の回りにある情報資産の監視体制の整備 ・利用者の身の回りにある情報資産の盗難防止策の整備	総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「サーバー室の情報セキュリティ対策」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin08.htm
・廃棄する際に、情報資産が流出しないよう、手順や履歴の管理を行っているか。	クライアントのハードディスクには、業務や教育研究活動において作られた情報が保存されています。これらを扱った機器類が廃棄される場合には、情報を適切に移行すると共に、重要度に応じて情報が確実に消去されるよう注意しなければなりません。特に、機器類をリースしていた場合等は、返却後に再利用される可能性があることを考慮して、重要な情報は確実に消去してから返却することが必要です。 また、機器類を廃棄する際には、その機器で利用していたソフトウェアのライセンスがどのような扱いになるのか確認し、適切に処理することが必要です。	・機器類の廃棄時に確実に消去すべき情報資産の明確化 ・情報を消去する手順の確立(実作業・証明書類) ・ソフトウェアライセンスの管理体制の整備	情報処理推進機構(IPA) ・情報セキュリティ:対策のしおり「情報漏えい対策のしおり ver.3」 http://www.ipa.go.jp/security/antivirus/shishi.html 総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策-実践編「コンピュータやメディアの廃棄」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_business/admin06.htm

チェックリスト項目	説明	対策例	関連資料
(4)情報媒体の管理	【狙い】 利用者が情報を持ち運ぶ際に使われる情報媒体(メディア)は、大容量化や使い勝手の良さから広く使われています。しかしながら、情報流出事故の多くが、このような情報メディアの紛失・盗難等によるものであることも事実です。 この部分では、利便性と機密性を考慮しなければならない情報媒体の取り扱いに対するチェックを狙いとしています。		
・情報媒体(USBメモリやハードディスクドライブ、ノートパソコン等)の持ち出しや持ち込みについて基準を設けているか。	USBメモリ・ハードディスクドライブ・ノートパソコン等は、使い勝手の良さから広く利用されていますが、大容量の情報を簡単に持ち運びできるので、情報漏えい事故の流出源にならないよう、取り扱いには十分な注意が必要です。 また、これらの情報媒体は、ウイルス等の悪意のあるソフトウェアの感染経路にもなりうるので、学内へ持ち込まれる際にも利用時にウィルスチェック等の対策が必要です。 保存されている情報の重要度により情報媒体の取り扱いの基準を設けたり、自動的に暗号化したり、そもそも情報を持ち出さなくても済むように利用環境・業務手順を見直す等の対策も検討が必要です。	・情報媒体の取り扱いに関するルール・ポリシーの作成 ・重要情報の取り扱いに関するルール・ポリシーの作成 ・暗号化ソフトウェアの導入 ・ウイルス対策ソフトウェアの導入 ・ネットワーク検疫システムの導入	平成20年度大学情報セキュリティ研究講習会 B.情報システム運用支援者コース 3.コンピュータ上の情報漏えい対策 情報処理推進機構(IPA) ・情報セキュリティ：対策のしおり「情報漏えい対策のしおり ver.3」 http://www.ipa.go.jp/security/antivirus/shishi.html 総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「持ち運び可能なノートパソコンを利用する上での危険性と対策」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin13.htm
・情報媒体はパスワード設定や暗号化等の紛失・盗難対策を講じているか。	重要な情報が保存されている情報媒体は、それ自身が情報資産であることを再認識する必要があります。十分な注意を払うのはもちろんのこと、紛失・盗難してしまった場合を想定し、重要度とリスクに応じた対策を施す必要があります。また、特に重要な情報については、自動的に暗号化することや、媒体として取り扱わずに済むように利用環境・業務手順を見直す等の対策も検討が必要です。	・暗号化ソフトウェアの導入 ・重要な情報を扱う利用環境や業務手順の見直し	平成20年度大学情報セキュリティ研究講習会 B.情報システム運用支援者コース 3.コンピュータ上の情報漏えい対策 情報処理推進機構(IPA) ・情報セキュリティ：対策のしおり「情報漏えい対策のしおり ver.3」 http://www.ipa.go.jp/security/antivirus/shiori.html 総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「持ち運び可能なメディアを利用する上での危険性と対策」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin14.htm
(5)情報施設・設備の管理	【狙い】 情報はネットワーク・サーバ・クライアント等の情報機器を利用して扱われます。利用者から見える・見えないに関わらず、これらの機器は適切な場所に設置しなくてはなりません。また、日常的に安定して運用するためには、電源や空調等の設備も整える必要があります。 この部分では、情報機器の可用性を高めるために必要な施設・設備に対するチェックを狙いとしています。		
・地震や火災等、施設に対する安全管理対策はできているか。	日本は地震大国であり、いつ何時どの地域でも地震に被災する可能性があります。不運にも被災してしまった場合に備えて、大学運営に関わる重要な情報資産が守れるように、また速やかにサービスを再開できるように考慮しなければなりません。情報システムを設置する建物・施設には、耐震構造であることや防火・消防機能を保有すること等が求められます。	・施設・設備・ファシリティ部門との連携 ・建物の耐震工事 ・防火・消防設備の見直し ・サーバラックへの機器の設置	総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「サーバーの設置と管理」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin06.htm
・電源や空調の安定運用、盗難防止等、設備や機器等に対する安全対策はできているか。	安定した電源の供給は、サーバ運用のための重要な基盤であり、停電や瞬断等に備えてUPS(無停電電源装置)を大いに活用するべきです。また、サーバ機器の集約度が高まっており、安定運用のためには、これらの機器からの廃熱を考慮して室温を制御する必要があります。機器類の盗難やいたずらの対策として、適切に設置されたラックにサーバ機器を収納することや入退室管理を行うことも重要です。情報システムを設置する部屋・領域には、適切な電源や空調設備、物理的な対策が求められます。	・電源環境の整備・見直し ・UPS(無停電電源装置)の導入 ・サーバ機器からの廃熱を考慮したサーバラック配置 ・サーバ機器からの廃熱を考慮した室温の制御 ・夏季の室温対策 ・入退室管理(鍵による管理・個人を特定した入退室履歴の管理) ・サーバラックへの機器の設置	総務省「国民のための情報セキュリティサイト」 ・情報管理担当者のための情報セキュリティ対策「機器障害への対策」 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin07.htm