別紙. 利用者別エンドポイントのセキュリティ対策（松竹梅）

利用者	利用形態	セキュリティ対策			備　　考
		松 システム的なセキュリティ対策 （端末にデータを保持しない）	竹 システム的なセキュリティ対策 （端末にデータを保持する）	梅 主に端末のセキュリティ対策	
職員	業務処理に利用	【ポリシー】 ・端末にデータを持たない（シンクライアント） 【対策】 ・画面転送型、端末型シンクライアント ・リモートアクセス型サービス	【ポリシー】 ・機器のセキュリティ対策と実施状況の管理まで実施 【対策】 ・検疫ネットワークの構築による、個別端末の監視 ・共通データの集約	【ポリシー】 ・端末のセキュリティ対策 【対策】 ・ウィルス対策、パーソナルファイアウォールなどの導入 ・ハードディスクの暗号化 ・共通データの集約	・組織的な対応が可能 ・業務の種類によっては、対応が困難な場合がある。例えば、施設系職員の業務など。
教員	教育・研究に利用 成績データの管理等業務に利用（成績情報等の重要なデータあり）	【ポリシー】 ・教育・研究用と業務用を分ける 業務用は、職員端末と同じ扱い 【対策】 1）教育・研究用 ・特殊な用途以外は、業務用と同等 ・特殊な用途のPCに対しては、「竹」、「梅」の対策 ・認証後にシンクライアント環境を仮想的に実行 2)業務用 ・画面転送型、端末型シンクライアント ・リモートアクセス型サービス	【ポリシー】 ・機器のセキュリティ対策と実施状況の管理まで実施 【対策】 ・検疫ネットワークの構築による、個別端末の監視 ・共通データの集約	【ポリシー】 ・端末のセキュリティ対策 【対策】 ・ウィルス対策、パーソナルファイアウォールなどの導入 ・ハードディスクの暗号化 ・共通データの集約	・教育/研究用と業務用を分ける ・学内からだけでなく、学外からの利用がある ・学外からのアクセス可能な情報の分離が必要 ・学外からは、重要度の応じて、画面転送、暗号化などを実施
学生	教育用PC（授業等で使用）	【ポリシー】 ・端末にデータを持たない（シンクライアント） 【対策】 ・画面転送型、端末型シンクライアント ・リモートアクセス型サービス	【ポリシー】 ・機器のセキュリティ対策と実施状況の管理まで実施 【対策】 ・ハードディスクキーパーなどによる改変阻止 ・検疫ネットワークの構築による、個別端末の監視	【ポリシー】 ・端末のセキュリティ対策 【対策】 ・ウィルス対策、パーソナルファイアウォールなどの導入	・不注意によるウィルス感染や不正侵入への対策が必要 ・被害の拡大が速い ・障害が発生すると、教育活動に支障が発生する ・学外からのアクセス可能資源の設定が必要
	持ち込みPC 研究室配属学生も同等？	【ポリシー】 ・学内では、学内用の環境を提供する 【対策】 ・認証後にシンクライアント環境を仮想的に実行	【ポリシー】 ・利用権限の確認と接続可能な端末の制限 【対策】 ・認証によって、利用権限を制限する。 ・検疫によって、ウィルス対策の実施状況などを確認する。	【ポリシー】 ・利用権限の確認 【対策】 ・認証によって、利用権限を制限する。	・端末がセキュリティレベルを決めてしまう ⇒マネジメントが必要
技術専門職員	教育・研究に利用	【ポリシー】 ・通常業務用と特殊業務用を分ける ・業務用は、職員端末と同じ扱い 【対策】 1）特殊業務 ・PCに対しては、「竹」、「梅」の対策 ・認証後にシンクライアント環境を仮想的に実行 2)通常業務 ・画面転送型、端末型シンクライアント ・リモートアクセス型サービス	【ポリシー】 ・機器のセキュリティ対策と実施状況の管理まで実施 【対策】 ・検疫ネットワークの構築による、個別端末の監視 ・共通データの集約	【ポリシー】 ・端末のセキュリティ対策 【対策】 ・ウィルス対策、パーソナルファイアウォールなどの導入 ・ハードディスクの暗号化 ・共通データの集約	・学内からだけでなく、学外からの利用がある ・技術力に大きなばらつきがある。
その他 （研究員、 名誉教授、 特任教授 客員教授）	教育・研究に利用	・研究教育用は研究室配属学生と同じ	・研究教育用は研究室配属学生と同じ	・研究教育用は研究室配属学生と同じ	・学内からだけでなく、学外からの利用がある ・業務は無いはず（業務用端末が必要ならば、事務職員と同等） ・研究室配属学生と同等
問題点と利点		〈問題点〉 ・インシデント発生時(サーバ)の影響が大 ・初期コストは大きい 〈利点〉 ・利用者によるリスクは低い ・セキュリティ管理の一元化 ・管理しやすい ・セキュリティ対策の一元化 ・予防のポイント、被害の規模が想定可能 ・対策状況を把握できる ・予防・処置の迅速性、徹底	〈問題点〉 ・利用者まかせのセキュリティ ・機器の紛失、データ持ち出しが可能 ・データ流出を防げない ・検疫に時間がかかる ・エージェントの場合、端末の多様性(OS)に対応できない ・被害の可能性が把握できない ・機器を持ち出したときに対応の必要性・データ持ち出しの危険性 ・起動が遅い(利便性の低下) 〈利点〉 ・認証を貫徹できる（利用者管理） ・ソフトウェアの管理が可能 ・今の利用形態と差が少ない ・端末ごとの多様性(Apps)を許容できる	〈問題点〉 ・利用者まかせのセキュリティ ・データ流出は防げない ・機器紛失、持ち出しが可能 ・対策が一元的にとれない ・強制が難しい ・管理が難しい ・被害の規模が把握できない 〈利点〉 ・簡単に始められる ・今の利用形態と差が少ない ・端末ごとの多様性(OS、Apps)を許容できる	
コスト		・短期的には投資額は高い ・中長期的には保守コストと効果で判断	・短期的にはある程度の投資が必要（梅のコスト+α） ・中長期的には保守コストと効果で判断	・短期的には投資額は低い ・中長期的にはは保守コストと効果で判断(高くなることもある) ・インシデント発生時のコストが高くなる可能性あり	新たな脅威に対し、継続的な投資が必要。