情報漏洩及び情報セキュリティ侵害の危険性が大きいソフトウェアの取り扱い要項

平成１８年９月１４日
情報企画推進委員会決定

（目的）

第１　本学情報セキュリティ対策基準 1.5「実施手順の作成」に定められた実施手順の一として、情報漏洩及び情報セキュリティ侵害の危険性が大きいソフトウェアの利用に関して全学的な取り扱いを定める。

（定義）

第２　この要項で、部局等とは各学部、大学院医歯学総合研究科、大学院連合農学研究科、大学院司法政策研究科、医学部・歯学部附属病院、附属図書館、保健管理センター、各学内共同教育研究施設及び事務局をいう。

（情報漏洩の危険性が高いファイル共有ソフトウェア等の取り扱い）

第３　別表１に示すファイル共有ソフトウェア等の利用は禁止する。ただし、各部局等の長が情報統括化責任者（CIO）に利用を申請し CIO がこれを許可した場合を除く。

（情報セキュリティを脅かす危険性の高いソフトウェア等の取り扱い）

第４　別表２に示すソフトウェア等を利用して学外から本来アクセスが許可されない学内のホストに対するアクセスを許可させ学外と学内を接続することは、ハードウェアが一体となった製品を利用する場合を含み禁止する。ただし、学術情報基盤センターが管理運営を行う VPN サービス及び各部局等の長が CIO に利用を申請し CIO がこれを許可した場合を除く。

（許可のないソフトウェア等の使用が確認された場合）

第５　前々項及び前項の CIO の許可のないソフトウェア等の使用が確認され、通信が継続している場合、学術情報基盤センターは CIO 及び当該部局等の長に通知を行った上で、163.209.0.1 から 163.209.255.254 のグローバル IP アドレスを持つホストについては当該ホストのグローバル IP アドレス、172.16.0.1 から 172.31.255.254 のプライベート IP アドレスを持つホストについてはそのホストの NAT 変換後のグローバル IP アドレスを対象に学外との全通信の遮断を実施する。

２　部局等に連絡がとれない等やむを得ない場合は、「鹿児島大学キャンパス情報ネットワークの運用管理に関する申し合わせ」の第７項（学術情報基盤センターの役割）に基づき、緊急遮断を実施する。

３　当該部局等の長が当該ソフトウェアの使用を停止させるとともに、CIO が解除を認めた場合に限り、学術情報基盤センターは遮断を解除する。なお、CIO は当該部局長に、再発防止対策を明記した遮断解除依頼書の提出を求めることができる。

別表１　ファイル共有ソフトウェア等

●WinMX、Napster など OpenNAP サーバを利用するファイル共有ソフトウェア
●LimeWire、Cabos、Gnutella など、Gnutella プロトコルを利用するファイル共有ソフトウェア
●Shareaza、iMesh など Gnutella2 プロトコルを利用するファイル共有ソフトウェア
●eMule、eDonkey、Morpheus など eDonkey ネットワークを利用するファイル共有ソフトウェア
●Kazaa など FastTrack ネットワークを利用するファイル共有ソフトウェア
●Winny、Winnyp など Winny プロトコルを利用するファイル共有ソフトウェア
●Share、Share UDP など Share プロトコルを利用するファイル共有ソフトウェア
●その他、ファイルを多数のユーザ間で共有することを目的としたソフトウェア

別表２　本来アクセスが許可されないホストに対するアクセスを許可させるソフトウェア等

●Softether、PacketiX VPN
●OpenVPN
●TinyVPN
●Hamachi
●その他、VPN 接続を可能にするソフトウェア及びハードウェア