写

１８文科総第９号
平成１８年４月２１日

各都道府県・指定都市教育委員会
各都道府県知事
各国公私立大学長　　殿
各国公私立高等専門学校長

文部科学省大臣官房長
玉井　日出夫

（印影印刷）

学校における個人情報の持出し等による漏えい等の防止について（通知）

学校が保有する個人情報については、個人情報の保護に関する関係法令及び各地方公共団体の条例等に基づき、適正な取扱いの確保に努めていただいているところですが、昨今、新聞報道等で、学校から持ち出された個人情報の漏えい事案が多く報じられています。

最近の傾向として、職員が許可無く職務上取り扱う個人情報を持ち出し、個人所有のパソコンを利用したことにより、ファイル交換ソフト等を介して流出するという事案が多く発生しています。

各位におかれては、学校における個人情報漏えい等の防止のため、既に諸々対策を講じられていることと思われますが、別添参考資料に示す①個人情報等の持出し、②学校外で利用するパソコンのセキュリティー、③ファイル交換ソフトへの対策を参考にして、個人情報の漏えい等の防止について適切に対応されるようお願いいたします。

なお、都道府県教育委員会及び都道府県知事におかれては、域内の市町村教育委員会、所管の学校及び所轄の私立学校等に対してご周知くださるようお願いします。

また、文部科学省ホームページにおいて、関連情報を提供しておりますので、適宜ご活用ください。

文部科学省ホームページ（関連情報提供ページ）：
情報の漏えい等の防止についての関連情報
http://www.mext.go.jp/b_menu/koukai/kojin/info.htm

【参考資料】

資料１「個人情報の持出し等による漏えい等の防止について（対策例）」
資料２「Antinnyの脅威」
資料３「昨今頻発しているWinny（ウィニー）利用による情報流出とは」
資料４「あなたは大丈夫？（今すぐできるセルフチェック）」
資料５「Winny及びAntinnyの検出・削除方法等」
資料６「対策参考リンク集」
資料７「情報管理体制チェックリストの参考例」

【本件照会先】
文部科学省大臣官房総務課情報公開・個人情報保護室
電話　03－5253－4111（内線2571）
大臣官房政策課情報化推進室（内線2251）

資料１

個人情報の持出し等による漏えい等の防止について（対策例）

１　個人情報等の持出しについて

（１）学校から個人情報等を持ち出す場合には、情報管理者の許可を得るなどのルールを明確化し、漏えい等（データの滅失、き損など）への防止対策を徹底する。

（２）電子メールにより非公表の情報を学校外へ送信する場合も、当該情報にパスワードを設定した上で送信するなど、必要に応じて保護対策を行う。

（３）個人情報の持出しによる漏えい事案では、教職員の認識不足によって発生する例が多いことから、漏えいの危険性について、教職員一人ひとりへ的確に周知を図るとともに、必要に応じて教育研修を実施する。

（４）大学等の教育研究活動において、学生等が個人情報を取り扱う場合においても、教職員と同様に安全管理措置等について周知し、適正な取扱いが確保されるよう必要な措置を講ずる。

２　学校外で利用するパソコンのセキュリティー対策について

（１）学校内で利用するパソコンのセキュリティ対策はもちろんのこと、学校外で業務に利用するパソコンについても、ウイルス対策ソフトがインストールされていることを確認するとともに、パターンファイルが最新の情報に更新されていることを確認する。

（２）ＯＳ等の脆弱性が改善されるよう、最新の修正プログラムを適用する。

（３）秘密情報、個人情報等の関係者のみが閲覧すべき情報については、パスワードで保護するなど、アクセス制限の措置を行う。

３　ファイル交換ソフト（Ｗｉｎｎｙ等）について

最近発生している情報漏えい事案では、学校外で利用したパソコンにファイル交換ソフト（Ｗｉｎｎｙ等）がインストールされており、コンピューターウィルスに感染したことによりパソコンに保存されていたファイルが漏えいする例が多数発生している。

このため、学校外で利用されるパソコンにファイル交換ソフト（Ｗｉｎｎｙ等）がインストールされていないことの確認を徹底する。

特に、自宅で利用する個人用のパソコンについては、以下の点に留意する。

①ファイル交換ソフトは、安易にインストールしないこと。

②ファイル交換ソフトの有無を点検し、これがインストールされたパソコンでは、児童生徒等の個人情報を扱わないこと。

③当該パソコンに、児童生徒等の個人情報等が保存されているか否かを点検し、保存されている場合は、適切に削除する等の措置をとること。

④ウィルスに感染した場合には、直ちに情報流出を遮断する措置を講ずること。

Winny 及び Antinny の検出・削除方法等の具体的手順

ファイル等を検索するための準備

Winny 及び Antinny の検出・削除を確実に行うためには、パソコンに記録されたすべてのファイルを検索対象にする必要があることから、管理者権限（ソフトウェアのインストール等を自由に行う権限）でログインする必要があります。

また、Windows では、隠しファイル、隠しフォルダ等を表示しない設定とされていると、これらを検索対象から除いてしまいます。Antinny に感染することにより作成されるファイルは、隠しファイル等にされていることが多いため、それらを検索するためには、すべてのファイルを検索対象とするための設定を行う必要があります。

さらに、実行形式のファイルを他の形式に偽装したウイルスを見分けるために、ファイルの拡張子についても、表示するように設定しておくことが望まれます。

Winny に係るファイルの検索 → Winny に係るファイルの削除

パソコンに記録されたすべてのファイルを対象として、ファイル名に「winny」を含むファイルの有無を確認します。Winny はパソコン上のどこにあっても使用することができることから、パソコン本体上のハードディスクに限らず、外部記憶装置についてもその存在の有無を確認してください。存在を確認した場合には、「winny」を含むファイル及び関連すると思われるファイルをすべて削除してください。

Antinny 感染の有無の確認 → Antinny の駆除

パソコンにウイルス対策ソフトを導入している場合は、パターンファイルを更新した上でパソコン(外部記録装置を含む。)に記録された全ファイルに対してウイルスチェックを実施することにより、当該パターンファイルが検出対象としている Antinny を検出することができます。

一方、パソコンにウイルス対策ソフトを導入していない場合でも、一部のウイルス対策ソフトメーカーのウェブページ上では、コンピュータウイルスを検出することができるサービスが提供されており、これを利用することにより、当該サービスが対象とする Antinny を検出することができます。しかしながら、このサービスではコンピュータウイルスの検出はできても、それを駆除することはできない場合がほとんどです。そのため、Antinny の感染を確認した場合には、ウイルス対策ソフトを利用するなどして、駆除を行う必要があります。

なお、ウイルス対策ソフト等により検出することができるコンピュータウイルスの範囲が異なり、検出することができない Antinny もあることから、ウイルス対策ソフト等を過信しないようにしましょう。

OS のクリーンインストール

Winny を使用した形跡又は Antinny の感染等が確認された場合には、当該パソコンには情報流出の危険性があります。また、上記の対策を実行したとしても、ウイルス対策ソフト等では検出することのできない Antinny もあるため完全に情報流出のおそれがないとは言い切れません。そのため、OS のクリーンインストールを実施することが望まれます。

【クリーンインストールとは】
ハードディスク上のソフトウェアやデータを完全に消去してから、ＯＳを再びインストールすること。なお、クリーンインストールした後は、ＯＳをアップデートして最新の状態にする必要がある。

※ 隠しファイルの表示方法、ファイル検索方法等については、対策連絡の資料を参照いただけると理解しやすいと思います。

※ クリーンインストールの実施においては、OS がインストールされていないドライブに Antinny が残されているおそれがあることにも留意すること。

資料２

*Winny*なんて使った覚えがないのに？！

あなたのパソコンから情報が流出していませんか？

～　Winnyの機能を悪用したコンピュータウイルス（Antinny）の脅威　～

○　Winnyをインストールしたパソコンが Antinnyに感染していると、パソコン（CD-R、USBメモリ等の外部記憶装置も含みます。）内に現在保存されている業務ファイル等のファイルのみならず、過去に一度でもそのパソコンで扱ったことがあるファイルがインターネット上に流出するおそれがあります。

○　一度流出した業務ファイル等を**インターネット上から完全に削除することは不可能**です。あなたの扱った業務ファイルやあなたの個人情報がインターネットを通じて多くの人の目に触れ、あなたは公私ともに大きな不利益を被るおそれがあります。

○　**Winny を一度でも利用したことのあるパソコンで業務ファイルを取り扱うことは極めて危険な行為**です。

「あなたは次々現れる Antinny の脅威に本当に対応できるのですか。
～ウイルス対策ソフトウェアの適切な利用はもちろん、様々な対策を迅速に講じなければ Antinny による情報流出を防ぐことは極めて困難です。」

○　あなたが Winny を利用した覚えがなくとも、家族と共に利用しているパソコンで業務ファイルを取り扱うことは、同様に極めて危険な行為です。

「あなたは、あなたの家のパソコンの利用状況を完全に把握できていますか？
～あなたの知らぬ間に**家族等が Winny を利用していませんか。**」

○　業務ファイル等の流出はあなたの組織にとどまらず、国民にも大きな不利益を与えます。**組織において業務ファイルの持ち出しに関するルールを再度よく確認し、職員の方は、これを確実に守って下さい。**

○　Antinnyに感染したパソコンから**業務ファイルを削除したり、ウイルス対策ソフトウェアを利用して Antinny を駆除するだけでは情報の流出は止まりません。**もし少しでも気がかりなことがあれば、できるだけ早期に**組織内の情報セキュリティ担当者等に相談して下さい。**

※　この種の情報流出は Winny を利用していない場合にも起こることがあります。

昨今頻発しているWinny(ウィニー)利用による情報流出とは

昨今頻発しているWinny（ウィニー）利用による情報流出とは、

①Winny（ウィニー）を利用しているパソコンが、

②コンピュータウイルス(Antinny（アンティニー）)に感染し、

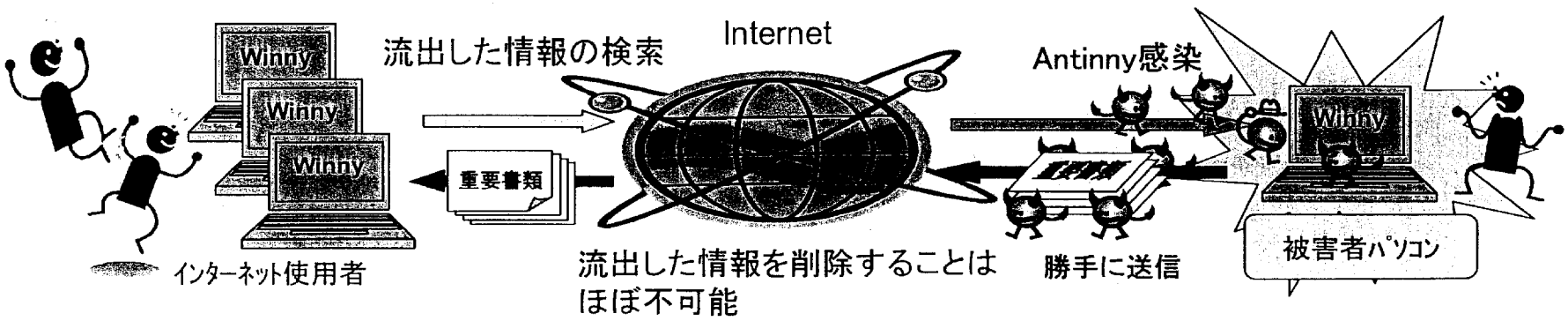
パソコン内にある外部に知られては困る情報が勝手にインターネット上に送信されたことにより発生。

Winny(ウィニー)とは

インターネットに接続したパソコン同士で音楽や画像などのデータを交換し合うファイル交換ソフトウェア

Antinny(アンティニー)とは

Winnyの機能を利用し、パソコン上のファイルを勝手にインターネット上に流出させるコンピュータウイルス
（Winnyの使用を原因として感染する場合が多い）



あなたは大丈夫？（今すぐできるセルフチェック）

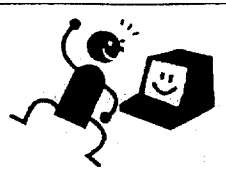
資料4

スタート

インターネットに接続したﾊﾟｿｺﾝに他人に知られたくない情報※を保存している。

定期的に確認してみましょう

※ 名簿、業務情報、ﾃﾞｼﾞｶﾒ画像、家計簿、電子メールやウェブページの閲覧履歴等のﾌﾟﾗｲﾊﾞｼｰ情報等

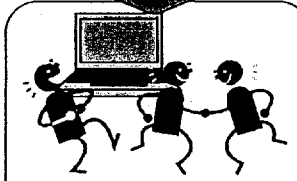


必要のない情報の削除等、万一の場合を考慮したﾘｽｸ軽減が必要

YES

NO

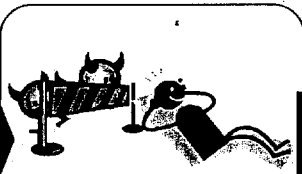
Yesには、「わからない」も含む。



ﾊﾟｿｺﾝを家族と共有している。

ファイル交換ソフトウェアWinnyを使用している。

OS及びｳｲﾙｽ対策ソフトの更新をしていない。



ｳｲﾙｽ対策ｿﾌﾄをｲﾝｽﾄｰﾙすれば安全だと思っている。

自分のﾊﾟｿｺﾝから情報が流出するはずがないと思っている。

（リスク）家族のﾌｧｲﾙ交換ｿﾌﾄ使用等を原因とする情報流出の危険性もあります。

（対　策）家族の使用状況をまず確認しましょう。また、家族に対して注意喚起をしましょう。

★確認の上、再度スタートに戻る

（リスク）ｳｲﾙｽ感染等を原因とする情報流出の危険性もあります。

（対　策）適時、OS及びｳｲﾙｽ対策ｿﾌﾄを更新することが望まれます。

（リスク）ｳｲﾙｽ対策ｿﾌﾄの使用・未使用に関わらず、Antinny等のｳｲﾙｽ感染を原因とする情報流出の危険性があります。

（対　策）他人に知られたくない情報をWinnyとﾊﾟｿｺﾝの双方が記憶媒体上で共存させないようにしましょう。Winny・Antinnyを削除するためにはﾊﾟｿｺﾝをﾘｶﾊﾞｰﾘｽﾄｰﾙすることが最も有効です。

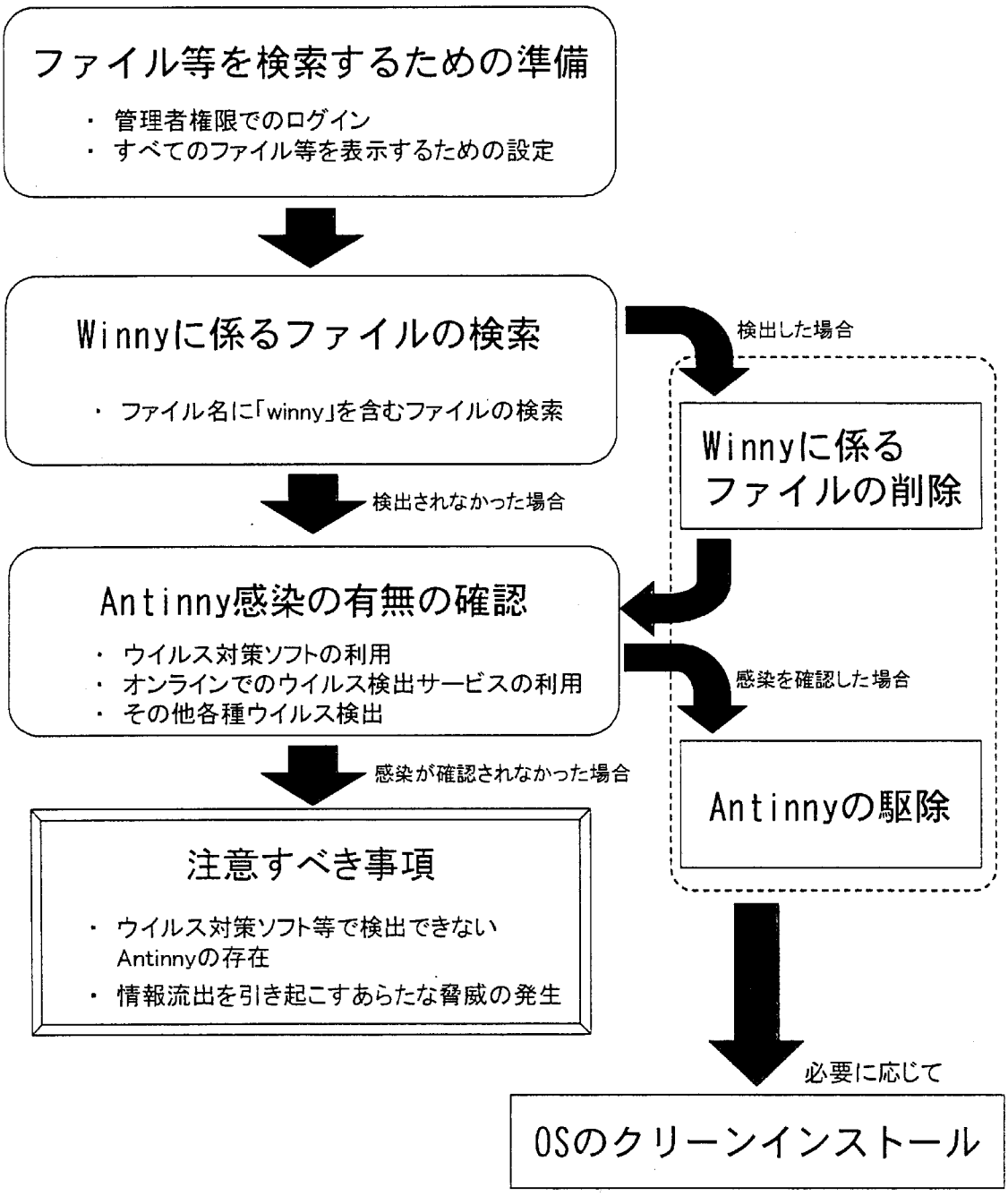
（リスク）ｳｲﾙｽ対策ｿﾌﾄが未対応であるｳｲﾙｽ等による情報流出の危険性もあります。

（対　策）完全な対策はないことを自覚し、他人に知られたくない情報については、暗号化等の取組みが望まれます。

Winny 及び Antinny の検出・削除方法等

ファイル交換ソフトウェア Winny の存在やコンピュータウイルス（Antinny）の感染の有無を確認し、対処する際の作業の流れを以下に示します。また、各項目における実施事項の詳細については、「Winny 及び Antinny の検出・削除方法等の具体的手順」に示します。

なお、コンピュータウイルスは、その種類により、検出や削除の方法等が異なるため、以下の方法は、すべてのコンピュータウイルスに対して有効な手段ではないことに留意して下さい。



資料6

☆☆対策参考リンク集☆☆

◎Winny/Antinny関係の注意喚起

①IPA 「Winnyによる情報漏えいを防止するために」
http://www.ipa.go.jp/security/topics/20060310_winny.html
「コンピュータウイルス・不正アクセスの届出状況[2月分]について」
http://www.ipa.go.jp/security/txt/2006/03outline.html

②Telecom-ISAC Japan 「T-ISAC-Japan Antinnyウイルス対策特設ポータルサイト」
https://www.telecom-isac.jp/news/news20060315.html

③マイクロソフト 「ファイル共有ソフトによる情報の流出について ~情報を手に入れるつもりが、情報を差し出すことに~」
http://www.microsoft.com/japan/athome/security/online/p2pdisclose.mspx

④ISSKK 「個人情報保護法施行後の情報漏えい事件について ～P2P ソフト Winny と、Antinny ウイルス～」
http://www.isskk.co.jp/security_center/winny.html

⑤トレンドマイクロ
「Winnyによる情報漏えい対策ページ」
http://www.trendmicro.co.jp/security/winny/
「ファイル交換ソフトWinny(ウィニー)による情報漏えいにご注意ください」
http://www.trendmicro.com/jp/security/report/news/archive/2006/vnews060302.htm

⑥LAC 「Winny（ウィニー）ファイル交換ネットワークの脅威」
http://www.lac.co.jp/business/sns/specialissue/winny.html

◎コンピュータウイルスの検知・駆除

①マイクロソフト 「悪意のあるソフトウェアの削除ツール」
http://www.microsoft.com/japan/security/malwareremove/default.mspx

②トレンドマイクロ
「ウイルスバスター オンラインスキャン」
http://www.trendmicro.co.jp/hcall/index.asp
「システムクリーナの使用方法（無償）」
http://www.trendmicro.co.jp/security/malwaremove/tsc/index.asp

◎Winnyがインストールされているかの検出

①LAC 「職場のＰＣセキュリティ診断サービス～企業内PCに潜むWinny（ウィニー）の存在を診断（無償）～」
http://www.shokuba-security.com/

資料７

情報管理体制チェックリストの参考例

１　基本的な対策のポイント

(1) 漏えいして困る情報を取り扱うパソコンには、ファイル交換ソフト（Winny等）を導入しない。

(2) 職場のパソコンに許可無くソフトウェアを導入しない、または、できないようにする。

(3) 職場のパソコンを外部に持ち出さない。

(4) 職場のネットワークに、私有パソコンを接続しない、または、できないようにする。

(5) 自宅に仕事を持って帰らなくて済むよう作業量を適切に管理する。

(6) 職場のパソコンからUSBメモリやCD等の媒体に情報をコピーしない、またはできないようにする。

(7) 漏えいして困る情報を許可無くメールで送らない、または、送れないようにする。

(8) ウイルス対策ソフトを導入し、最新のウイルス定義ファイルで常に監視する。

(9) 不審なファイルは開かない。

２　管理対策上の点検項目例（パソコン利用のルールができていますか？）

(1) 学校、事務所、研究室等で使用するパソコンのセキュリティ対策状況（ウイルス対策状況、修正プログラム適用状況）を把握しているか？

(2) 個人情報や機密情報等の外部への持ち出しについてのルールを定めておく。

①個人情報や機密情報等を含む業務情報を記録媒体などにコピーして外部に持ち出すことについてルールはあるか？

②持ち出しが認められていない情報が含まれていないか？

③記憶媒体などにコピーされて外部に持ち出された個人情報や機密情報等を管理できるか？

(3) 私有パソコンの利用条件を定めておく。

①私有パソコンを職場に持ち込んで使用したり、職場のネットワークに接続することについてのルールを定めているか？

②私有パソコンを利用することを許可制にしているか？

③私有パソコンを職場から持ち出す場合のチェックは十分か？

(4) 教職員へウイルス対策の重要性を再認識させる。

①Winny等による情報漏えい事件の主な発生要因を十分理解させているか？

②自分は大丈夫だ、自分には関係ないということは間違いであることの意識改革をさせているか？

③セキュリティ対策製品やサービスも完全ではないことを理解させているか？

(5) ファイル交換ソフトの使用条件を定めておく。

①研究用途など、限られた業務において必要ということでファイル交換ソフトを使用しているパソコンはないか？

②ファイル交換ソフト及びファイルの管理は充分に行っているか？

（実際は、完全なウィルスへの対策は不可能であるといわれており、ファイル交換ソフトを安易に使用しない。）

3　技術対策上の点検項目例（技術上の対策はできていますか？）

(1) 重要情報に対するアクセス制限を設けているか？

(2) 重要な情報に対するコピー制限を設けているか？

(3) 重要な情報を暗号化しておくための対策ができているか？

(4) USBメモリ、CD-R、FD、MOなどの記録媒体の利用制限を設けているか？

(5) 私有パソコンの職場内ネットワーク接続に制限を設けているか？

＊この情報管理体制チェックリストの参考例は、独立行政法人情報処理推進機構セキュリティーセンター（ＩＰＡ）の資料をもとに作成しました。詳しくは、資料６「対策リンク集」のＩＰＡ「Winnyによる情報漏えいを防止するために」をご参照ください。

＊この情報管理体制チェックリストの参考例は、機関ごとのルールに応じて利用してください。