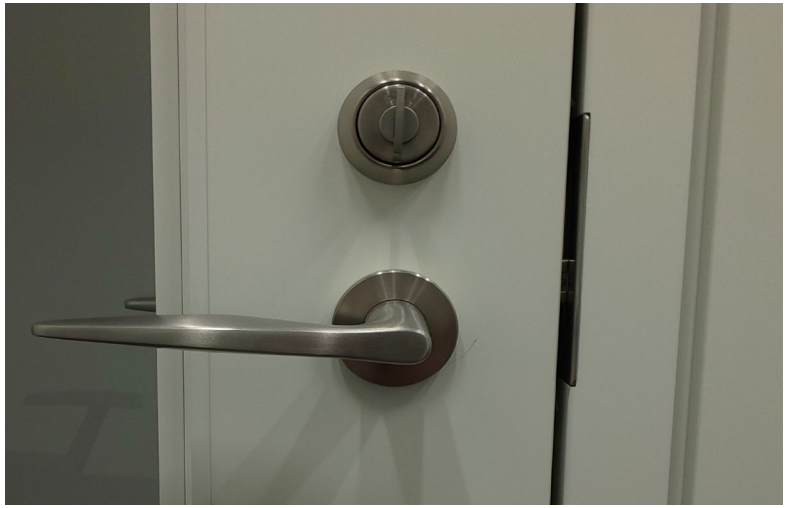
JROAD　国循外データ利用に関する Q&A

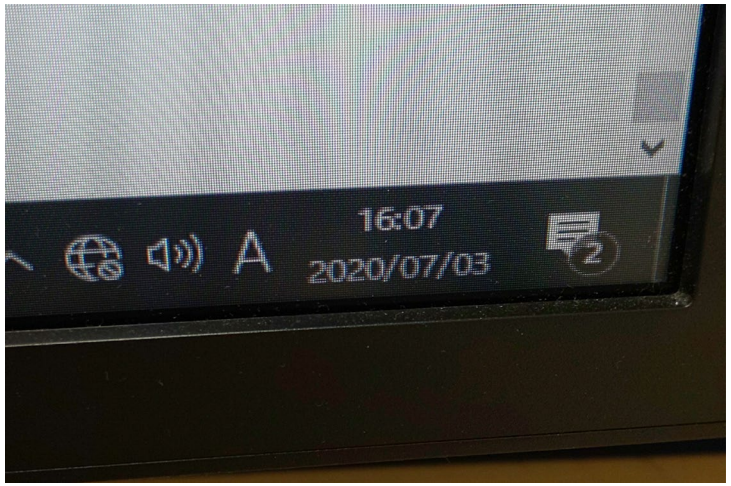
2020/7/6　ver.1.0

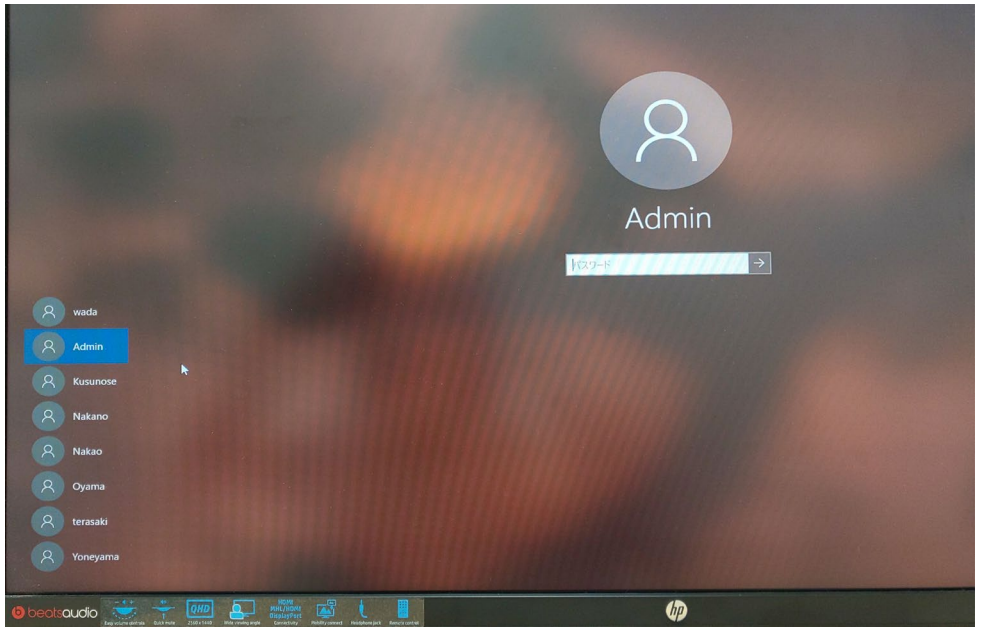
Q1.解析室用のお部屋はどのような対応が必要ですか？

＝＞JROAD解析室の対応状況は以下のように個室・施錠可能となっています。
入退室を台帳やノートで記録してください。



Q2.個室・PC・アカウントはどのような管理が必要ですか？





個室に解析用PC（ディスクトップ・ノート）を設置。
PCは、日付と時刻を調整する。
アカウントは、解析者別の作成してください。
パスワードは定期的に変更（最長でも2 ヶ月以内）、
極端に短い文字列を使用せず英数字、記号を混在させた
8 文字以上の文字列とし、類推しやすいパスワードを使用
しないこととする

Q3.PCの盗難防止用にどのような対応が必要ですか

個室では、PCの持ち出しができないように
盗難防止用チェーンを用いて
PCと机を固定するなど工夫する。
ノートパソコンも同様の対応をしてください。

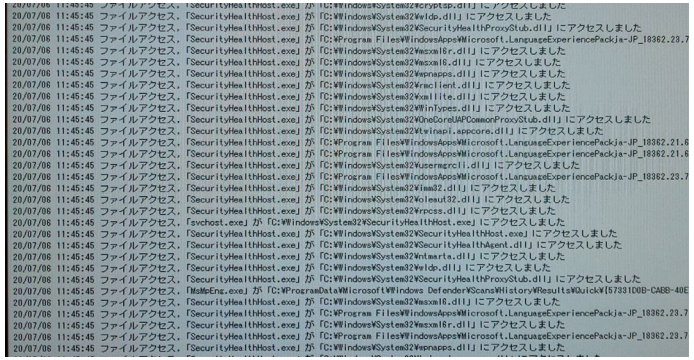
Q4.解析結果持ち出しはどのように実施しますか？

持ち出しに使用する情報機器（USB等）は、
①ウイルスを自動で検知・隔離できる「ウイルスチェック機能」搭載
②第三者の利用を防止するためにパスワードによるセキュリティーが設定（盗難、置き忘れ等に対応する措置）
以上の条件を満たすものを利用する。

Q5.解析用端末のログ管理、PCロック、データの暗号化、セキュリティソフトの更新が必要とされていますが、どのように対応すればよいでしょうか？

下記にようなPCログ管理・ストレージ利用制限・データ暗号化用のソフトやスタンドアロンPC用のセキュリティ対策用USB導入をご検討ください。

①PCのロック
②機密データの暗号化
③USBストレージの利用制限
④操作ログの記録、参照



スタンドアロンPCのセキュリティ対策

スタンドアロン/クローズド環境端末の定期チェック

USBメモリ型の検索ツールを対象端末に挿すだけで、ソフトウェアのインストールを行うことなく（※1）、最新のパターンファイル（※2）でウイルスチェックを行えるため、定期チェックを手軽に行うことが可能です。

※1 ウイルス検索時に、一時的に検索対象端末にドライバおよびローカルHDDにファイルを作成しますが、検索終了後、検索対象端末に当該ドライバおよびファイルは残りません。（USBブート検索を行った際、ログを検索対象端末のローカルハードディスクに作成するか選択可能です）検索対象端末にTMPS2を挿入した際、パターンファイル更新やウイルス検索の自動実行を行う場合は、検索対象端末に検索ツールエージェントをインストールしておく必要があります。

JROAD公募研究　国循外データ提供時チェック項目一覧

No	管理要件	チェック項目
1	＜セキュリティ要件＞	利用・保管場所　→あらかじめ申し出られた施錠可能で入退室管理を行っているスペースのみとなっているか
2		提供情報を複写した情報システム・機器はインターネット等の外部ネットワークには接続していないか
3		提供情報は事前に申し出られた利用者以外の者が利用していないか→確認方法担保：情報システムの認証、アクセス情報のログ監視・管理の措置
4	＜組織としての管理対策＞	学部、研究室、研究チームの合理的な範囲内でガイドライン等のルールを定めた運用管理規程の確認
5	＜人的安全対策＞	申請があった場合のみ：所属する組織以外の外部業者に委託する場合（例えば、PCの修理など）、受託業者との守秘契約の締結や作業内容確認（作業計画、作業報告など）の運用ルールの確認
6	＜運用管理の対策＞	提供情報が保存されているPC等、機器の設置場所、清掃業者等、委託業者の出入りの確認
7		JROADデータを使用する端末は盗難防止用チェーンを設置しているか
8		利用場所の開錠・施錠時刻と開錠・施錠を行った者のログ情報（生体認証）の確認、または台帳管理された内容の確認
9		成果物持ち出しを行う場合に使用するUSBなどの記録媒体は、それを保存するラックなどは施錠管理されているか
10		USBメモリ等には、管理番号等を付番し、台帳等で所在場所などを管理し、紛失時の情報漏えい等を防ぐ観点から当該USBメモリ等には、パスワードを設定され、定期的に変更がおこなわれているか
11	＜技術的な対策＞	JROADデータ等を利用する情報システムへのアクセスにおける利用者の識別と認証の確認
12		利用者がJROADデータ等を利用する情報システムの端末から長時間、離席する際、あらかじめ認められた利用者以外の者が利用する恐れがある場合には、クリアスクリーン等の防止策を講じているか
13		JROADデータ等を利用する情報システムへのアクセスの記録及び定期的なログの確認おこなっているか（アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した利用者が特定できることが必要）
14		JROADデータ等を利用する情報システムにアクセス記録機能がない場合はのみ 業務日誌等で操作の記録（操作者及び操作内容）の確認
15		JROADデータ等を利用する情報システムにアクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じているか

No	管理要件	チェック項目
16		アクセスの記録に用いる時刻情報は信頼できるものであるか？→情報システムの時刻表示のチェック
17		原則としてJROADデータ等を利用する情報システムには、適切に管理されていないメディアを接続していないか確認。ただし、システム構築時、やむをえず適切に管理されていないメディアを使用する場合、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認しているかを質問する
18	＜パスワードを利用者識別に使用する場合＞	利用者がパスワードを忘れたり、盗用されたりする恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録をしているかの確認
19		システム管理者であっても、利用者のパスワードを推定できる手段を防止しているか（管理者への確認）
20		利用者は、パスワードは定期的に変更し（最長でも2 ヶ月以内）、極端に短い文字列を使用していないか（英数字、記号を混在させた8 文字以上の文字列が望ましく、類推しやすいパスワードを使用しないこと）
21	＜データ利用終了時の対応＞	JROADデータ等の利用の終了後には、情報システム内に記録されたJROADデータ等及び中間生成物を消去することに加え、消去後に当該機器を外部ネットワークに接続する際にはあらかじめコンピューターウイルス等の有害ソフトウェアが無いか検索し、ファイアウォールを導入するなど、安全対策に十分配意しているか
22	＜情報及び情報機器の持ち出し＞	提供されたレセプト情報等の利用、管理及び保管は、事前に申し出られた場所でのみ実施しているか
23		外部への持ち出しは行わないこと。※ただし、外部委託や共同研究の場合など、やむをえず、あらかじめ申し出られた利用者の間で最小限の範囲で中間生成物等の受け渡しを行う場合には、利用者が以下の23-1~23-6の措置を講じ、JROADデータ等の受け渡しに準用されているか
23_1		組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程の確認
23_2		運用管理規程には、持ち出した情報及び情報機器の管理方法を定められているかの確認
23_3		情報を格納した媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程等に定められているかの確認
23_4		あらかじめ運用管理規程等で定めたJROADデータ等の盗難、紛失時の対応を従業者等に周知徹底し、教育を行っているか
23_5		利用者は、JROADデータ等が格納された可搬媒体もしくは情報機器の所在を台帳管理しているか
23_6		JROADデータ等の持ち出しに利用する情報機器（USB等）に対して起動パスワード設定の確認。（盗難、置き忘れ等に対応する措置として、JROADデータ等に対して暗号化、アクセスパスワードを設定する等、容易に内容を読み取られないようにするため設定にあたっては推定しやすいパスワード等の利用を避け、定期的にパスワードを変更する等の措置を行う。）
23_7		JROADデータ等が保存された情報機器を、他の外部媒体と接続する場合は、コンピューターウイルス対策ソフトの導入を行う等して、情報漏えい、改ざん等の対象にならないような対策を施すこと。