北海道大学
情報基盤センター
システム適正利用の手引き

2019 年 3 月 20 日版

北海道大学情報基盤センター

本手引きの目的

近年，情報システムへの不正アクセス，情報漏洩，データ改ざんなどのセキュリティインシデントが世界的に数多く発生しています。その予防のため，適切なアカウント・パスワード管理，システム管理・監視，セキュリティアップデートの適用など，基本的な対策を徹底して行うことが重要です。

本手引きは，北海道大学情報基盤センターが提供する大型計算機システム（スーパーコンピュータシステム，クラウドシステム，ストレージシステム等）の利用者を対象とし，その利用にあたり特に留意すべき点を，パブリッククラウドサービス（事業者が提供する商用のサービス）との対比も含めてまとめたものです。特に，クラウドシステムについては，利用者がサーバの管理者権限を持ち，その環境すべてを管理・運用することから，セキュリティについて十分な注意を払って運用することが求められます。**センターが提供するシステムの利用にあたっては，事前にすべての項目をご熟読いただき，遵守くださるようお願いいたします。**本手引が安心してシステムをご利用いただくための一助となれば幸いです。

利用上の注意

1. 本文書は随時改訂されますので，必ず最新版を参照するようにしてください。
   （掲載 URL　https://www.iic.hokudai.ac.jp/tebiki/）
2. 本文書は，特に留意すべき点を示したものであり，ページ数の制約などから想定される全ての状況をカバーしたものではありません。また，例示された各サービスの内容や提供条件が変更となる場合がありますので，本文書に加えて，関連規程や各種通知など，本センター及び関係組織等から提供される情報を必ず確認し，適正な情報システム利用を心がけてください。

スーパーコンピュータシステム・アプリケーションサーバ

情報基盤センターが提供するスーパーコンピュータシステム，アプリケーションサーバの概要及び，特に注意すべき点について，以下に示します。

1. **スーパーコンピュータシステム**：大規模な科学技術計算のための計算資源を，電気代相当の負担金で提供しています。その利用にあたっては，適切なパスワードを設定するとともに，その管理を厳重に行ってください (p.6 を参照)。

2. **アプリケーションサーバ**：研究向けのアプリケーションソフトウェアを実行するためのサーバで，大型計算機システムの基本負担経費のみで利用できます。その利用にあたっては，適切なパスワードを設定するとともに，その管理を厳重に行ってください (p.6)。

3. 外国籍の方がスーパーコンピュータシステムを含む大型計算機システムを利用する場合，安全保障輸出管理に係る手続きが必要となりますので，詳細について必ず事前に利用者窓口（hsay@iic.hokudai.ac.jp）までお問い合わせください。

4. アプリケーションサーバで利用いただける商用ソフトウェアについては，一部の例外を除き北海道大学所属の教職員および学生に限定されていますのでご注意ください。また，利用者がライセンスを保有するソフトウェアをスーパーコンピュータシステムやアプリケーションサーバにインストールして利用する際は，ライセンス契約上可能かどうか，利用者の責任で確認の上，ご利用ください。

5. **スーパーコンピュータシステム**および**アプリケーションサーバ**のストレージには，利用申請時に記載した研究課題に関わるデータ，原則としてスーパーコンピュータおよびアプリケーションサーバで利用する研究データのみを置くことができるものとします。**また，極めて高い重要度を有し、漏洩や改竄等が生じた場合に深刻かつ重大な影響を及ぼす情報（マイナンバー、入試情報、成績情報、診療記録等）については、本サービスによる取り扱いを禁止します。 (p.7)。**

クラウドシステム・クラウドストレージ

クラウドシステム・クラウドストレージについて特に注意すべき点を以下に示します。

1. **クラウドシステム（移行用サーバを含む）**：研究向けの計算用サーバを想定した物理サーバ及び仮想サーバを提供しています。研究用のシステムを想定したサービスですので，サーバ環境のバックアップは利用者の責任で行ってください。

2. **クラウドシステム**の利用にあたっては，サーバの管理者権限を利用者が持つことになります（技術的理由から，情報基盤センターでは個々のサーバの管理者権限を持てません）ので，**利用者の責任で適切なサーバ・ネットワーク管理(p.4) を行うことが必須となります。外部業者に構築，運用などを委託する場合も最終的な責任は利用者にあります (p.10) 。**さらに，登録される全てのアカウントについて適切な管理が必須となります(p.5)。また，本サービスを利用して保存、処理、公開等されるデータについては、利用者の責任において管理し、その重要度（機密性、完全性、可用性）に応じて適切な取り扱い（暗号化、二重化、監視やバックアップなど）を行うものとします。また、極めて高い重要度を有し、漏洩や改竄等が生じた場合に深刻かつ重大な影響を及ぼす情報（マイナンバー、入試情報、成績情報、診療記録等）については、本サービスによる取り扱いを禁止します。(p.7)。

3. **クラウドストレージ**： Dropbox のようなクラウドストレージを大容量かつ高速な学内設置のストレージシステムとして提供しています。大型計算機システムの基本負担経費のみで 100GB（学生は 10GB）まで追加料金無し（それ以上は利用負担金を支払うことで，1TB 単位で追加可能）で利用できます。インターネット経由でファイルのアクセスができますので，その**パスワードの取り扱いには特に注意してください（p.6）。また，極めて高い重要度を有し、漏洩や改竄等が生じた場合に深刻かつ重大な影響を及ぼす情報（マイナンバー、入試情報、成績情報、診療記録等）については、本サービスによる取り扱いを禁止します。 (p.7)。**

適切なサーバ・ネットワーク・アカウント管理

クラウドシステムのプロジェクトサーバ，ホスティングサーバの管理・運用に当たっては，サーバの管理権限全てを利用者側が持つことから，管理できるすべての要素（OS，ソフトウェア，アカウント，パスワード，データなど）について管理責任を有することを十分意識し（サービスごとの責任分界点については p.11 を参照），特に以下の点に注意してください。

1. セキュリティ脆弱性に対応するため，**ソフトウェアのアップデートを必ず実施してください。**ソフトウェアとしては，OS に加えて，各種ソフトウェア，ライブラリ，ミドルウェアなどについても適切に行う必要があります。これらには Web サーバプログラム（Apache など），PHP などのライブラリ， CMS（Wordpress など），分散処理環境（Hadoop など）も含まれます。多くのソフトウェアでは自動更新の設定がありますので，**特に不都合がない場合は，自動更新とすることをお勧めします。**（自動更新で不都合が生じることもありますので，その場合は利用者の責任で管理してください。）

2. サーバのネットワークについて，不必要なポートは全て遮断する，送信元を最小限に絞るなど，適切なファイアウォール設定を行ってください。また，SSL に対応するためのサーバ証明書が必要な場合は，国立情報学研究所が提供する UPKI 電子証明書発行サービスの証明書が追加費用なしで使えますので，利用者窓口（hsay@iic.hokudai.ac.jp）までご相談ください。

3. 適切な暗号化（PPTP など脆弱性が指摘されている古い方式は使用しないでください）を用いた VPN（仮想プライベートネットワーク）を用いることで通信経路中の安全性を向上させることができますが，サイト間 VPN などで送信元，受信先からさらに他のネットワークに接続されている場合，不正通信やコンピュータウィルスが伝搬されるなど予想外の波及効果が生じる可能性がありますので，十分注意して運用してください。

4. 研究開発用の試験システムや機密性の高い情報を取り扱うシステムなど，**リスクの高いシステムについては，ファイアウォールの設定においてアクセス元を最小限に限定し**，その限定されたアクセス元端末などからアクセスする際は，適切な暗号化を用いた VPN や鍵認証による SSH など安全性の高い方法を用いるようにしてください。

5. 新規にアカウントを登録する場合には，その利用者に対して，適切なパスワードの管理（p.6）など，適正利用についてご指導ください。**卒業，異動などにより利用されなくなったアカウントについては速やかに削除する**などアカウントの管理を徹底してください。また，しばらく利用しないアカウントについては，ロックをかけるなどの対応をお願いします。スーパーコンピュータシステムについては以下の手順でロックをかけられます：

   利用者管理ポータル -> サービスメニュー -> スーパーコンピュータ -> 情報登録・参照 -> アカウントロックの変更

6. 外国籍の方に対してサーバのアカウントを発行する場合，安全保障輸出管理に係る手続きが必要となりますので，詳細について必ず事前に利用者窓口（hsay@iic.hokudai.ac.jp）までお問い合わせください。

7. アカウント管理については，OS に加えて，各種ソフトウェア，ミドルウェアなどについても適切に行う必要があります。これらには，Web サーバプログラム（Apache など），コンテンツマネジメントシステム（Wordpress など），分散処理環境（Hadoop など）も含まれます。**ソフトウェアによっては，デフォルトのアカウントに安易なパスワードが付されている恐れもありますので，十分注意してください。**

8. 利用者がライセンスを保有するソフトウェアをクラウドシステムのサーバにインストールして利用する際は，ライセンス契約上可能かどうか，利用者の責任で確認の上，ご利用ください。

9. 不正ログインなどのインシデントがあった場合にできるだけ速やかに発見するため，定期的にアクセスログ，ネットワークログなどをチェックし，**不審なログインや通信があった場合には直ちに情報基盤センター大型計算機システム CSIRT（hpc-security@iic.hokudai.ac.jp）へ連絡してください。速やかな発見・報告が被害の拡大を防ぐ上で極めて重要です。**

適切なパスワード・鍵管理

大型計算機サービスの利用，サーバへのアクセスに必要となるパスワードなどの認証情報について，特に以下の点に注意し管理してください。

1. 利用しているサーバ，サービスに関わる全てのアカウントについてパスワードが脆弱なものとなっていないか（長さは十分か，数字や特殊文字を含めているか，辞書に登録されている安易なキーワードを用いていないか，など）**サーバ，サービスの対象ユーザ全員に徹底してください。特に管理者パスワードについては，高い強度のパスワードを設定するとともに，絶対に漏洩することのないよう，厳重に管理してください。**また，他のシステムやサービスのパスワードと同じものを用いることは絶対にしないでください。

2. 代表的な遠隔端末操作手段である SSH でサーバへアクセスする場合，送信元 IP を限定せずアクセスする，重要情報を取り扱うシステム，大規模・複雑なシステムであるなど，リスクが高いと判断される場合はパスワード認証を無効化（/etc/ssh/sshd_config で PasswordAuthentication no と設定する）し，鍵認証を用いてください。鍵のパスフレーズについては上記のパスワードに準じて設定し，**パスフレーズ無しの鍵は絶対に用いないでください。**鍵の管理は厳重に行い，秘密鍵が漏洩しないよう最大限の注意を払ってください。

適切な情報・データ管理

1. 取り扱う情報の格付けをもとに，適切な対応をしてください。例えば**要機密情報については暗号化をするとともに所属組織外へ絶対に持ち出さない**など，それぞれの情報の所有者（組織）で定められている規則を事前に必ず確認してください。（北大関係者が取り扱う情報については「国立大学法人北海道大学における情報資産の格付け及び取扱制限に関する内規」を事前に必ず確認してください。）なお，北海道大学情報基盤センターが提供する大型計算機システムには，入試問題などの試験関連情報，成績などの個人情報，診療情報など，**最高レベルの機密性を有する情報は絶対に保存しないでください。**（その場合，インターネットから隔離された専用システムや端末，北海道大学においては事務クラウドなどをご利用いただくことになります。）

2. プライバシー情報などの個人情報については，特に厳重な管理を行うとともに，**医療分野など対象分野ごとにガイドラインが定められている場合は，必ずそれにしたがった対応をしてください。また，輸出管理規制に該当する情報についても，許可なく国外へ持ち出さないなど特段の注意を払ってください。**

3. 研究データについては，研究不正対応のため**原則として成果発表後１０年間保存することが求められています。**データの保存について，一義的には研究者本人の責務ですが，情報基盤センターにおいてクラウドストレージを提供しておりますので，必要に応じてご活用ください。また，パブリッククラウドを利用する場合は，機密情報に該当しないかどうか，暗号化は施されているか，などの検討を行った上で十分注意してご利用ください。

4. クラウドシステム，サービスを用いてデータを保存する場合，一つのシステム，サービスを全面的に信頼せず，異なるシステム，サービスにまたがってバックアップを取ることを強くおすすめします。これは，不正アクセスによるシステムやサービスの乗っ取り，ランサムウェア（感染するとデータを強制的に暗号化するなどアクセスできなくする悪意のあるソフトウェア）などで，データへのアクセスができなくなった場合にも有効となることがあります。

5. 情報やデータのアクセス権限，公開設定について適切な管理を行ってください。**設定を誤ると意図しない情報流出・漏洩にもつながりますので，十分注意してください。**

通信制限解除申請について

現在，包括的セキュリティ対策により北大外からの通信は原則遮断されています。北大外から北大内のサーバなどへのアクセスが必要となる場合，北海道大学情報環境推進本部情報セキュリティ対策室宛に「インバウンド通信制限解除申請」を行ってください。申請もしくは申請に関する問い合わせについては， qa@csc.hokudai.ac.jp までメールでご連絡ください。

1. 申請に当たっては，必要とされる最小限のアプリケーション名及び TCP/UDP ポート番号並びに送信元を指定し，送信元を不特定（CIDR 表記で 0.0.0.0/0 ）とすることはできる限り避けてください。
   （全世界の理論上最大４３億台の機材に対して当該ポートを公開することになりますので， https（443 番）ポートなど真に必要な場合に限定してください。）

外部委託（アウトソース）する場合の注意点

クラウドシステム上において，システム構築，運用などの作業の一部または全てを外部の業者等に委託する場合，**全体的な責任はあくまで作業を委託する利用者側にあり**，その責務の一部を契約に従って委託しているに過ぎない，ということを十分認識の上，特に以下の点に注意してください。

1. 情報の取り扱いやセキュリティ対策など，**どの部分を外部の業者に委託したことになっているのか，その契約でカバーできず利用者側で行うべき部分はどこか，などの切り分けについて明確にしてください。**例えば，ホームページの構築を依頼する際，コンテンツ作成のみ依頼しサーバ管理やセキュリティ対策などの運用部分について契約に含まない場合は，サーバの運用管理，セキュリティ対策などについては，利用者側で責任を持って行う必要があります。

2. 作業を委託する業者の選定についても，委託する利用者側の責任となります。プライバシーマークなどの第三者認証を取得しているか，実績はどうか，などを十分検討し，単にコストのみで判断しないよう注意してください。委託契約を行う際の仕様策定にあたっても，セキュリティポリシーの遵守，格付けに応じた情報の取り扱いなど，必要なセキュリティ要件を必ず記載してください。

3. 北大所属の教職員が委託契約を含む情報システム関連の調達を行う際，情報システム最適化申請が必要となる場合があります。（学外クラウドの調達については必ず申請が必要となります。）その条件など詳細については，以下の本学情報環境推進本部情報システム最適化のページ（学内限定）をご参照ください。

   http://ict.general.hokudai.ac.jp/hp-file/sub4.html

責任分界点（サービス提供側と利用者側の責務の境界）について

情報基盤センターが提供する大型計算機システムに関わる各サービスの提供条件を，パブリッククラウド（事業者が提供する商用のクラウドサービス）との対比も含めて以下に示します。それぞれの情報システム・サービスごとに，その提供者側の責務が規定されており，利用者側の責務との共有により全体としてセキュリティが保たれます。**サービス利用者の管理下にある情報やシステムのセキュリティを確保する最終責任は利用者自身にある**ということを十分認識し，サービス提供側の条件を確認しつつ利用者側の責務を果たすことが求められます。

サービス	サービス提供側の責務	サービス利用者側の責務
情報基盤センター スーパーコンピュータシステム アプリケーションサーバ	ハードウェア，オペレーティングシステム，ジョブスケジューラ，アプリケーションソフトウェア	適切なアカウント，パスワード，データ管理，適正な資源利用など
情報基盤センター クラウドシステム （物理サーバ，GPU サーバ）	ハードウェア（サーバ，ネットワーク，ストレージ，など）	適切なオペレーティングシステム，ソフトウェア，データ，アカウント，パスワード管理，サーバ監視，など
情報基盤センター クラウドシステム （仮想サーバ，移行用サーバ）	ハードウェア，ハイパーバイザ，クラウド管理ソフトウェア	適切なオペレーティングシステム，ソフトウェア，データ，アカウント，パスワード管理，サーバ監視，など
情報基盤センター ストレージシステム （スパコン・クラウド）	ハードウェア（ストレージ，ネットワーク），ストレージ管理ソフトウェア	適切なアカウント，パスワード，データ管理，機密情報の暗号化，アクセス権限設定，など
パブリッククラウド（サーバやストレージなどのシステム基盤やプラットフォームを借りる場合）	サービス事業者の提供条件（通常，ハイパーバイザ，クラウド管理ソフトウェアまで）	その他全て（オペレーティングシステム，ソフトウェア，データ，アカウント，パスワード管理，サーバ監視，など）
パブリッククラウド（Web サービスを利用する場合）	サービス事業者の提供条件	その他全て

参考情報（URL，メールアドレス）

北海道大学情報基盤センター　https://www.iic.hokudai.ac.jp/

・大型計算機システムポータル　https://www.hucc.hokudai.ac.jp/

・大型計算機システム利用者窓口　hsay@iic.hokudai.ac.jp

・大型計算機システム CSIRT　hpc-security@iic.hokudai.ac.jp

（大型計算機システムに係るセキュリティインシデントの連絡先）

北海道大学情報環境推進本部　http://ict.general.hokudai.ac.jp/ （学内限定）

・情報セキュリティ対策室　qa@csc.hokudai.ac.jp

（通信制限解除申請に関する問い合わせ・送付先）

・北海道大学 CSIRT　security@iic.hokudai.ac.jp

（大型計算機システム以外の北海道大学に係るセキュリティインシデントの連絡先）

北海道大学情報基盤センター

システム適正利用の手引き

2019 年 3 月 20 日

https://www.iic.hokudai.ac.jp/tebiki/

本手引きに関する問合せ先

hsay@iic.hokudai.ac.jp
