ユーザー情報セキュリティガイドライン

以下の条項は、プラズマシミュレータ（PS）の全てのユーザーに対して有益なユーザーデータの基本的保全方法や安全な使用方法について記載しています。

ユーザーの属するコンピューターセンターや管理部門の指示事項は、本条項より優先されます。したがって、ユーザーが特異な状況下において本ガイドラインの有効性や有益性に疑念を持った場合、ユーザーの所属機関のコンピューター管理者に問い合わせ、指示を受けてください。

1　アクセス制約条件

1.1　アカウントについて

1.1.1　ユーザーは自分のログイン ID を他人に使わせてはならない。また他人のログイン ID を用いて PS にアクセスしてはならない。

1.2.1　ユーザーは所属機関等の登録情報が変更となるときは速やかに連絡すること。

1.2　パスワードについて

1.2.1　見える場所にパスワードを書かない。

1.2.2　その他のシステムに同じパスワードを使用しない。

1.2.3　故意にあるいは偶発的に他のユーザーにパスワードを開示しない。

1.2.4　ブラウザにパスワードを記憶させない。

1.3 ローカルセキュリティについて

1.3.1　PS に接続している時は PC から離れない。少なくとも、仕事場所を離れる時はパスワードプロテクトスクリーンセーバーにする。

1.3.2　何らかの理由でスクリーンを共有し、PS にログインしている場合、使用後は PS セッションを直ちに閉じる。PS にログインしている間は共有スクリーンを離れない。

1.4 トレーニングについて

1.4.1　PS 利用のために必要と思われるいかなるトレーニングや登録にも進んで参加する。

2　接続される機器の構成

2.1　オペレーティングシステムについて

2.1.1　サポートの終了したオペレーティングシステムは使用しないこと。

2.1.2　使用するオペレーティングシステムには最新のセキュリティアップデートをする。

2.2　ウイルス等対策について

2.2.1　常に最新版のウイルスチェックソフトウェアを使用する。

2.2.2　オペレーティングシステムに関係なく、独自の機器使用によるマルウェアの偶発的起動に警戒する。ファイルを開く場合、メールに添付された疑わしいソースに特に注意する。（機器やデータにダメージを与えるだけでなく、記録され、そしてキーストロークが伝達される様々なマルウェアがある）

2.2.3　PS へアップロードするファイルがマルウェアを含まないよう注意する。

2.2.4　PS へ繋がるいかなる機器のソフトウェアの変更も PS ネットワークやシステムに

ダメージを与える、若しくはセキュリティ脆弱化の原因となってはならない。

2.3 ポートについて

2.3.1　スヌーピングや攻撃に対してシステムを脆弱にする可能性のあるポートを開ける時は注意すること（例：外部からの FTP アクセス）。また、機器への遠隔ログインは、特定のユーザーのみを許可するようにすること。パスワードキーチェーン等はパスワードにより守られるようにすること。

3　接続された機器のデータとソフトウェアの防御について

3.1　PS に繋がるどんなソフトウェアも最新版にアップデートする。特に PS に繋がるために関わるブラウザ。

3.2　PS オペレーターはデータの損失やダメージを防ぐようにするが、いかなるデータの損失やダメージに対してもその金銭的責任を負わないことに注意せよ。

3.3　携帯メディアからのウイルスやマルウェア感染のリスクに注意する。

3.4　データキャリアの修復や廃棄に関連するリスクの可能性に注意する。

4　セキュリティリスクについて

4.1　ユーザーは自分のアカウントに対する不正アクセスの兆候がないか注意し、懸念事項があった場合は、ユーザーサポートにメールにより報告する。

4.2　PS オペレーターは以下の権限を持つことに注意せよ。ユーザーが実行するあらゆるプログラムの一時停止をすること。一時停止が続行される前にそれに関わる詳細な情報を PS オペレーターに提供することをユーザーへ要求すること。

5　もし機器が攻撃された場合

5.1　直ちに PS からログアウトし、ブラウザを閉じる。

5.2　ネットワークの攻撃から防御するため、インターネット（ワイヤレス、イーサネット）から機器をはずす。

5.3　ユーザーが属する IT 管理者に速やかに報告し、修復の際はその指示に従う。