

利用規定

2021年7月

本利用規定(以下「AUP」という。)は、お客様及びお客様の代理人が、当社が提供するオンラインサービス(以下「クラウドサービス」という。)を利用する際に遵守する必要があります。条件を定めています。

1. 認証情報

お客様は以下を遵守します。

- 虚偽の ID を使用してクラウドサービスにアクセスしない。
- アクセス認証情報やセキュリティトークンは厳重に保管し、不正にアクセス、開示、使用されないように保護する。
- クラウドサービスにアクセスする場合は、お客様のユーザーアカウントを使用するなど、必ず当社が許可している方法でアクセスする。
- お客様のユーザーアカウント、基盤技術、又はこれらに関連するホスト、ネットワーク、アカウントの認証情報又はセキュリティを無効にしたり開示したりしない。
- すべてのアクセス認証情報は他者と共有しないようにし、認証情報が付与されている個人のみが使用するようにする。合理的裁量に基づいて変更が必要であると判断した場合、当社はアクセス認証情報を変更することがある。

2. 違法、有害、攻撃的な使用やそのようなコンテンツの禁止

お客様はクラウドサービスを違法、有害、攻撃的な用途に使用したり、他者に対してそのような使用を喚起、奨励、促進、容易にしたり、指示したりしないようにします。また、違法、有害、不正、侵害的、攻撃的なコンテンツを送信、保存、表示、配布、又はその他の方法で利用可能な状態にしたりしないようにします。お客様によるクラウドサービスの使用と、クラウドサービス内に保存されるお客様のコンテンツについては、以下を遵守する必要があります。

- 法律や規制に違反したり、他者の権利を侵害したりしない。
- 詐欺的な商品、サービス、商法、プロモーション、一攫千金商法、ねずみ講、マルチ商法、フィッシング、ファームिंग、その他の欺瞞的な行為を提供、流布を含め、他者又は当社の評判を損なうことはしない。
- 自身のコンテンツ又はコンテンツの一部として、権限が付与されていないコンテンツ又は不正なコンテンツのハイパーリンクを入力、保存、送信したり、そのようなコンテンツが含まれている外部の Web サイト又はデータフィードへのアクセスを、埋め込みウィジェットなどのアクセス手段を含め、有効にしたりしない。
- 誹謗中傷、わいせつな表現、罵詈雑言、プライバシーを侵害する表現、その他の好ましくない内容は回避する。

3. 使用制限の遵守

お客様は以下を遵守します。

- クラウドサービスの再販売、譲渡、サブライセンス許諾、貸与、リース、公開を行ったり、ビジネスプロセスアウトソーシングなど、アウトソーシングやタイムシェアリングサービスの運営にクラウドサービスを利用したりしない(ただし、当社が明示的に許可した場合を除く)。
- クラウドサービス又はその基盤技術のソースコードをリバースエンジニアリング、逆アセンブル、逆コンパイルしたり、ソースコードのマージ、改ざん、修復に

よって製品の変更、派生製品の作成、もしくはソースコードの解明を行ったりしない(この制限がお客様の法域の適用法に抵触する場合を除く)。

- 適用される法的制裁措置及び/又は(再)輸出管理に関する法律と規制に従い、法的制裁措置又はライセンス要件によって禁止又はその対象となっている場所からクラウドサービスにアクセスしない。これは欧州連合、米国及び/又はその他の当該国が含まれる。適用される(再)輸出管理法によって許可されていない場合、又は個々の政府により認可又は承認されていない場合、お客様は非管理対象コンテンツのみをアップロードする(例: EU の分類番号は「N」、米国の分類番号(ECCN)は「N」又は「EAR99」)。

4. 乱用の禁止

お客様は以下を遵守します。

- クラウドサービスに規定されている使用制限や制約(アクセス制限、ストレージ制限など)、監視、又は料金の発生を無効又は回避するような方法でクラウドサービスを使用しない。
- 性能試験の実行、競合製品や競合サービスの構築、機能やユーザーインターフェースのコピーを目的として、クラウドサービスにアクセスしたり、クラウドサービスを使用したりしない。当社のシステムの適切な機能やセキュリティを妨害しない。
- 迷惑となる大量の一斉メールやその他のメッセージ、プロモーション、広告、勧誘(商業広告や情報告知を含む)を配布、公開、送信、促進しない。送信者の明示的な許可を得ることなく、メールのヘッダを変更又は不明瞭にしたり、送信者の ID を推測したりしない。

5. セキュリティ違反の禁止

お客様は、クラウドサービス又はその基盤技術のセキュリティ侵害を発生させたり促したりするような方法で、クラウドサービスを使用しないようにします。お客様は特に以下を遵守します。

- お客様のシステム、オンサイトのハードウェア、ソフトウェア、又はお客様がクラウドサービスへの接続及び/又はアクセスに使用するサービスを標的としたセキュリティ攻撃、ウイルス、悪意なコードに対して妥当な予防措置を講じる。
- 当社の書面による明示的な同意を得ずにクラウドサービス又はその基盤技術に対する侵入テストを行わない。
- 業界標準のセキュリティポリシー(パスワード保護、ウイルス対策、更新及びパッチのレベルなど)に準拠していないデバイスを使用して、クラウドサービスにアクセスしたりクラウドサービスを使用したりしない。

6. 当社のモニタリング、報告、監査

お客様は、当社及び当社の協力会社が、お客様の本 AUP の遵守状況を、クラウドサービスを通じてモニタリングする可能性があることを了承します。当社は、本 AUP に対する違反行為を調査する権利を有します。お客様が本 AUP に対する違反行為に気付いた場合、お客様は直ちに当社に通知し、当社の要請に応じて、違反行為の停止、軽減、是正に協力します。当社、当社の協力会社又は委任代理人は、事前に妥当な通知を行った上で、お客様の構内、ワークステーション、サーバーにおいて、お客様が本 AUP を遵守しているかどうかを監査することがあります。当社は、本 AUP 又はクラウドサービスの利用に関して当社がお客様と交わしたその他の契約に違反するコンテンツ又はリソースを削除、アクセス不能、又は変更することがあります。当

社は、法律又は規制に違反していると思われる活動を、適切な法執行当局、規制当局、又はその他の適切な第三者に報告することがあります。お客様によるクラウドサービスの利用又はお客様のコンテンツが、第三者の権利又は法律や規制に違反すると当該第三者が主張する場合、当社は適切な顧客情報を共有することがあります。

7. **著作権/DMCA.** シーメンスは、コンテンツに関する著作権侵害の通知に対して、著作権ポリシーに基づいて対応します。著作権ポリシーについては、www.siemens.com/sw-terms/dmca に記載されています。