制定日：2026 年 10 月 21 日

ProPlus＋セキュリティに関する補足規約

この規約は、ProPlus+のセキュリティに関して、ProPlus＋利用規約を補足する規約（以下「本補足規約」といいます。）です。ユーザーは、ProPlus＋利用規約とあわせて本補足規約に従い ProPlus＋のサービスを利用する必要があります。ProPlus＋利用規約と本補足規約の内容との間に相違がある場合は、本補足規約の内容が優先するものとします。また、本規約で用いる用語は、本補足規約で別途定めるものを除き、ProPlus＋利用規約と同一の意味を有するものとします。

1. 本補足規約の目的
本補足規約は、ProPlus＋利用規約を補足し、ProPlus＋上にユーザーが登録した業務データおよびマスターデータ（以下ユーザーデータという。）に係る取り扱いおよびセキュリティについて定めるものです。

2. ユーザーデータの管理
プライバシーに関する法令の遵守
ProPlus＋は、本サービスに一般的に適用されるすべてのデータ保護およびプライバシーに関する法令を遵守します。ただし、特定のカテゴリのデータまたはユーザーもしくはユーザーの業界に適用されるデータ保護およびプライバシーに関する法令で、情報技術サービスプロバイダーには適用されない法令についてはこの限りではなく、プロシップはその遵守に関しては、責任は問われないものとします。

3. ユーザーデータの削除
プロシップは、本サービスの契約管理者が利用終了手続を行った場合に、ProPlus＋上からユーザーデータを削除します。また、利用条件に違反する形で、本サービスが利用停止となってから相当の期間が経過した場合にも、ユーザーが利用終了手続きを行ったとみなし、ユーザーデータを削除します。ユーザーの登録データの削除はプロシップの責任で行い、削除されたユーザーデータは、プロシップもまた復旧することができません。削除条件、削除時期および削除対象となるユーザーデータは、次のとおりとします。
削除条件：契約期間終了後 6 か月以内
削除対象：ProPlus＋上にユーザーが登録したデータ（業務データおよびマスターデータ）

４．ユーザーの責任
・ユーザーは、本サービスの使用に関連して適用される、プライバシー、データ保護および通信の秘密に関する法的要求事項に従う必要があります。
・ユーザーは、次のセキュリティ対策を実施する必要があります。
a. 各ユーザーに付与されたパスワードの適切な管理
b. ProPlus＋におけるアカウントの適切な管理（登録、削除、管理者権限の付与など）

５．セキュリティ
(1) 技術的および組織的セキュリティ体制
プロシップは、ユーザーデータの漏えい、滅失、毀損その他の不正なアクセス、損失または破壊を防止し、またはその影響を軽減するため、合理的かつ適切な技術的・組織的安全管理措置を講じ、これを継続的に維持、点検、評価および更新する。これには、アクセス制御、暗号化、不正プログラム対策、CSIRT の設置を含む。これらのセキュリティ体制におけるプロシップの責任はユーザーデータのセキュリティおよび取扱い（不正アクセスと漏洩の防止）に限定され、ユーザーデータの守秘義務については、ProPlus＋利用規約に定めるところによるものとします。

(2) セキュリティインシデント
ProPlus＋に保管されているユーザーデータへの違法なアクセス、または当該機器もしくは施設に対する不正なアクセスによるユーザーデータの消失、開示または改変（以下それぞれについて「セキュリティインシデント」といいます。）が発生したことが判明した場合、プロシップは、(a) ユーザーにセキュリティインシデントを通知し、(b) セキュリティインシデントを調査してその情報をユーザーに報告し、(c) セキュリティインシデントの影響を軽減し、損害を最小限にするための妥当な対策を実行します。

ユーザーは次の事項に同意するものとします。
セキュリティインシデントが失敗に終わる場合は、前号は適用されず、プロシップの調査義務、通知報告義務および対策実行義務は発生しません。この場合においてセキュリティインシデントが失敗に終わる場合とは、ユーザーデータまたはユーザーデータを保管している ProPlus＋に対する不正なアクセスが発生しなかったインシデントで、ファイアウォールまたはエッジサーバーへの ping 攻撃またはブロードキャスト攻撃、ポートスキャン、失敗したログオン試行、サービス拒否攻撃、パケットスニッフィング（または、IP アドレスまたはヘッダーより後のデータにアクセスされなかったトラフィックデータへのその他の不正アクセス）などが含まれます。

上掲のセキュリティインシデントに対するプロシップの報告や対応は、セキュリティインシデントに関して過失責任、賠償責任その他の責任をプロシップが負うものと認めることを意味するものではありません。
セキュリティインシデントが発生した場合、72 時間以内を目安として、プロシップの選択に基づき、電子メールその他の 1 つまたは複数の手段によりユーザーの管理者に通知されます。
また、セキュリティインシデントを発見した場合の報告、または情報セキュリティインシデントに関する問い合わせは、ProPlus＋サポート窓口や貴社担当 CS など、顧客担当窓口にて受け付けます。

６．データの暗号化
ProPlus＋では、製品およびサービス全体で信頼性・堅牢性の高い Amazon Web Services を使用しており、データの暗号化を実施しております。また、複数の暗号化方式、プロトコル、アルゴリズムを使うことにより、データがインフラストラクチャを通過する際に利用できるセキュリティで保護された経路を提供し、インフラストラクチャ内に保存されたデータの機密性を保護しています。

7. ユーザー登録データの保管場所
ProPlus＋では、日本国内の Amazon Web Services 上にユーザーが登録したデータを保管しています。

8. データのバックアップ
ProPlus＋では、Amazon Web Services 上にて保管期間(7 日程度)の任意の時点にリカバリ可能な継続的バックアップの仕組みを利用してバックアップを取得しております。

9. 知的財産権に関する問い合わせ
知的財産権に関する問い合わせは、ProPlus＋サポート窓口や貴社担当 CS など、顧客担当窓口にて受け付けます。

以上