データ処理契約

本データ処理契約(以下「本契約」という。)は、Siemens Product Lifecycle Management Software Inc.、別名Siemens Industry Software(以下「SISW」という。)と、本契約の条件に同意することを表明したお客様(以下「お客様」という。)の間で締結されます。 SISWは、本契約に基づく権利を行使し、義務を遂行するために、関連会社を利用する権利を保持します。 したがって、本契約で用いられる「SISW」という用語は、Siemens Product Lifecycle Management Software Inc.の最終的な親会社によって直接又は間接に所有又は支配され、Siemens Product Lifecycle Management Software Inc.によってSISWクラウドサービス(以下「クラウドサービス」という。)を提供する権限を与えられた関連会社を指すことがあります。

お客様は、処理の影響を受けるデータの種類及び関係者の決定について全責任を負うものとし、クラウドサービスを用いた当該処理の合法性を保証するものとします。 お客様は、クラウドサービスによって提供される機能を使用した、個人データのあらゆる修正、削除、又は遮断に対しても責任を負うものとします。 お客様は、クラウドサービスによって提供される機能を使用して、個人データを含め、そのデータをエクスポート及び削除することができます。 本データ処理契約が解除により終了した場合、お客様は30日の間、お客様データをお客様がダウンロードできるようにすることを、書面によりSISWに要求するものとします。 当該要求に応えてSISWによって定められた期間の満了後、お客様の残りのデータは、削除の対象となり、お客様は利用することができなくなります。 SISWとお客様は、クラウドサービスの範囲内で、お客様の指示発行権が、クラウドサービスによって提供される機能のみを使用して行使されることに合意します。 お客様のデータに関する追加指示には、当該指示の遂行のためお客様によって支払われる追加料金に関する契約を含めた、SISWとお客様の間の個別の書面による契約が必要です。 SISWとお客様がクラウドサービスでの保護医療情報(PHI)の保管を明示的に許可する別個の書面による契約を締結していない限り、お客様は、いかなるPHIもクラウドサービスにアップロード又は保存しないことを誓約します。

クラウドサービスを提供する際、生産システムに関して、SISWは、本データ処理契約の別紙Aの付録2に記載された技術的及び組織的な対策に従うものとします。 クラウドサービスに関連する非生産システムは、別紙Aの付録2に記載されている対策に従う場合と従わない場合があります。これに加えて、SISWは、生産システムに適用される技術的及び組織的な対策を随時変更することができます。但し、当該変更が、当該対策によって得られる保護のレベルに具体的に悪影響を及ぼす場合はこの限りではありません。 SISWは、その従業員に対して個人データを許可なく収集、処理、又は使用することを制限し、データプライバシー保護要件に従って具体的に指示されたお客様の個人データの処理にのみ従業員を雇用します。

SISWは、クラウドサービスの遂行に準処理者を従事させる権利を有するものとします。 準処理者によるお客様の個人データへのアクセスを排除できない限り、SISWは、当該準処理者とその各所在地のリストを要求に応じてお客様に提供し、新規準処理者がお客様の個人データへのアクセスを許可される前に、必要に応じて当該リストを更新します。 お客様が新規準処理者に対して妥当な異議申し立てを行う場合、お客様は、当該異議をSISWに通知し、SISWが新規準処理者の雇用を主張した場合、本データ処理契約を正当な理由をもって解除する権利を有するものとします。 当該準処理者の雇用に個人データの国境を越えた移転が関わる限りにおいて、SISWは、当該準処理者が当該個人データに関するデータ保護の適切なレベルを維持できるように努めます。

SISWは、適用される技術的及び組織的な対策の順守を定期的に確認し、お客様からの妥当な要求に応じて、適用される技術的及び組織的な対策が順守されていることをお客様に対して確約します。 お客様は、SISWによる確認が誤りであると信じるに足る根拠を有する場合、妥当な事前通告がある場合に限り、SISWと監査の取り決めを行うことにより、技術的及び組織的な対策の順守を確認する権利を有するものとします。 当該監査の実施費用は、お客様が負担するものとします。

SISWとお客様は、欧州連合内の国から、EUが個人データ保護の適切なレベルを保持していないと見なすEU域外の国への、お客様の個人データのデータ転送が、別紙Aに規定され、本契約に完全に組込まれているEU標準契約条項の規定に従って実施されることに合意します。 本データ処理契約の条件と標準契約条項の条件に矛盾がある場合、標準契約条項の規定が優先されます。 標準契約条項は、データ輸出者(別紙Aで定義)が設立されたEU加盟国の法律によって支配されます。

別紙A
EU標準契約条項

適切なレベルのデータ保護を確保していない第三国で設立された処理者への個人データの移転に対する95/46/EC指令の第26条(2)項について

両者

お客様及び/又はEU内に拠点を置くお客様の関連会社

(以下「**データ輸出者**」という。)

と

Siemens Product Lifecycle Management Software Inc.の最終的な親会社によって直接又は間接に所有又は支配され、Siemens Product Lifecycle Management Software Inc.によって代理でデータを処理する権限を与えられた関連会社を含む、Siemens Product Lifecycle Management Software Inc.、別名Siemens Industry Software

(以下「**データ輸入者**」という。)

それぞれ「当事者」、両者を総称して「両当事者」は、

付録1で指定された個人データのデータ輸出者によるデータ輸入者への移転に関して、個人のプライバシー、基本権及び自由の保護に関する適切な予防対策を提示するため、以下の契約条項(以下「条項」という。)に合意します。

第1条。　定義

条項における定義:

(a) 「個人データ」、「特別カテゴリーのデータ」、「プロセス/処理」、「管理者」、「処理者」、「データ主体」及び「監督機関」は、個人データの処理に対する個人の保護と当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の95/46/EC指令で定められた定義と、同じ意味を有するものとします。

(b) 「データ輸出者」とは、個人データを移転する管理者を意味します。

(c) 「データ輸入者」とは、移転後にデータ輸出者に代わって、その指示と条項の条件に従って処理することを意図した個人データを、データ輸出者から受領することに同意しており、且つ95/46/EC指令の25条(1)項に規定する範囲内で適切な保護を確保する第三国のシステムの適用を受けない処理者を意味します。

(d) 「準処理者」とは、移転後にデータ輸出者に代わって、その指示、条項の条件及び書面による契約の条件に従って処理業務を実行することのみを意図した個人データを、データ輸入者又はデータ輸入者のその他の準処理者から受領することに同意している、データ輸入者又はデータ輸入者のその他の準処理者によって雇用された処理者を意味します。

(e)「適用されるデータ保護法」とは、個人の基本的権利と自由、及び特にデータ輸出者が設立された加盟国のデータ管理者に適用される個人データの処理に関するプライバシーの権利を保護するために制定された法律を意味します。

(f)「技術的及び組織的なセキュリティ対策」とは、特に処理にネットワーク経由のデータ送信が含まれる場合の偶発的又は違法な破壊又は不慮の損失、改変、無許可の開示又はアクセス、並びにその他のすべての不法な形式の処理から個人データを保護することを目的とした対策を意味します。

第2条。　移転の詳細

個人データの移転及び該当する場合は特に特別カテゴリーの個人データの詳細が、条項の不可欠な部分である付属文書を形成する付録1で指定されています。

第3条。　第三受益者条項

1. データ主体は、第三受益者として、データ輸出者に対して本条項、条項4(b)～(i)、条項5(a)～(e)、(g)～(j)、条項6(1)と(2)、条項7、条項8(2)、及び条項9～12を強制することができます。

2. データ輸出者が事実上消滅するか、又は法律上存在しなくなった場合、データ主体は、データ輸入者に対して本条項、条項5(a)～(e)と(g)、条項6、条項7、条項8(2)、及び条項9～12を強制することができます。但し、任意の承継法人がデータ輸出者のすべての法的義務を契約又は法律の運用によって承継し、その結果としてデータ輸出者の権利と義務を引受けた場合はこの限りではありません。この場合、データ主体は、当該法人に対してこれらの条項を強制することができます。

3. データ輸出者とデータ輸入者の双方が事実上消滅するか、法律上存在しなくなるか、又は支払い不能になった場合、データ主体は、準処理者に対して本条項、条項5(a)～(e)と(g)、条項6、条項7、条項8(2)、及び条項9～12を強制することができます。但し、任意の承継法人がデータ輸出者のすべての法的義務を契約又は法律の運用によって承継し、その結果としてデータ輸出者の権利と義務を引受けた場合はこの限りではありません。この場合、データ主体は、当該法人に対してこれらの条項を強制することができます。 準処理者の当該第三者責任は、条項に基づく準処理者自身の処理操作に限定されるものとします。

4. データ主体が明示的に希望する場合、且つ国内法令によって認められる場合には、両当事者は、データ主体が1つの団体又はその他の組織によって代表されることに対し異議を申し立てないものとします。

第4条。　データ輸出者の義務

データ輸出者は、以下に同意し保証するものとします。

(a) 移転自体を含む、個人データの処理が、適用されるデータ保護法の関連規定に従って実行されてきており、今後も引続き実行されること(且つ、該当する場合は、データ輸出者が設立された加盟国の関連機関に通知されていること)、その国の関連規定に違反していないこと。

(b) 移転される個人データをデータ輸出者に代わって、適用されるデータ保護法と条項に従ってのみ処理することを、データ輸入者にこれまでも指示しており、今後も個人データ処理サービスが継続する間、指示すること。

(c) データ輸入者が、本契約の付録2に指定された技術的及び組織的なセキュリティ対策に関する十分な保証を提供すること。

(d) 適用されるデータ保護法の要件の評価後、特に処理にネットワーク経由のデータ送信が含まれる場合の偶発的又は違法な破壊又は不慮の損失、改変、無許可の開示又はアクセス、及びその他のすべての不法な形式の処理から個人データを保護するセキュリティ対策が適切であること、且つこれらの対策により、先端性及び実装費用に関して、保護対象データの処理と特質によってもたらされるリスクに対し適切なセキュリティのレベルが確保されること。

(e) セキュリティ対策の順守を保証すること。

(f) 移転に特別カテゴリーのデータが関係する場合、95/46/EC指令の意味の範囲内で適切な保護を提供しない第三国にデータが送信される可能性がある移転の前、又は移転後できるだけ早い時期に、データ主体に通知されていたか、又は今後通知されること。

(g) データ輸出者が移転の継続又は一時停止の解除を決断した場合、条項5(b)及び条項8(3)に従ってデータ輸入者又は準処理者から受取った通知をデータ保護監督機関に転送すること。

(h) 付録2を除いた条項のコピー及びセキュリティ対策の概要記述、並びに準処理サービスの契約のコピーを要求に応じてデータ主体が利用できるようにすること。これは、条項に従って作成する必要があります。但し、条項又は契約に商業情報が含まれる場合はこの限りではありません。この場合、これらの商業情報を除去することができます。

(i) 準処理の際、条項に基づいてデータ輸入者が提供する個人データ及びデータ主体の権利の保護のレベル以上のレベルで、処理業務が準処理者によって条項11に従って実行されていること。

(j) 条項4(a)～(i)の順守を保証すること。

第5条。　データ輸入者の義務

データ輸入者は、以下に同意し保証するものとします。

(a) 個人データをデータ輸出者に代わって、その指示と条項に従ってのみ処理すること。何らかの理由で当該順守を実践できない場合、順守できない旨をデータ輸出者に速やかに伝えることに同意します。この場合、データ輸出者は、データの移転を一時停止及び/又は契約を解除する権利を有します。

(b) データ輸入者に適用される法律が、データ輸出者から受取った指示及びデータ輸入者の契約上の義務の遂行を妨げると信じる理由がないこと、及び本立法に、条項によって提供される保証及び義務に実質的に悪影響を及ぼす可能性がある変更があった場合、認識時に直ちにデータ輸出者に速やかに変更を通知すること。この場合、データ輸出者は、データの移転を一時停止及び/又は契約を解除する権利を有します。

(c) 移転された個人データの処理前に、付録2で指定された技術的及び組織的なセキュリティ対策が実装されていること。

(d) データ輸出者に以下について速やかに通知すること。

(i) 法の執行機関からの個人データの開示に対する法的拘束力を持つ要求(法執行機関の捜査の機密性を保持するための刑法に基づく禁止など、通知することが禁止されている場合は除きます)。
(ii) 偶発的又は不正なアクセス
(iii) まだ応答していない、データ主体から直接受取った要求(直接の応答を許可されている場合は除きます)。

(e) 移転の際の個人データの処理に関するデータ輸出者からのすべての問合わせに迅速且つ適切に対処し、移転されたデータの処理に関する監督機関の助言に従うこと。

(f) 条項の対象となる処理業務の監査のため、データ処理施設を提示するようデータ輸出者から要求された場合に応えること。監査は、データ輸出者、又は独立したメンバーから成る、必要な専門的な資格を備え、且つ守秘義務によって拘束され、該当する場合は監督機関の同意を得て、データ輸出者によって選ばれた検査機関によって履行されるものとします。

(g) 条項又は既存の準処理サービス契約のコピーを、条項または当該契約に商業的な情報が含まれていない限り、要求に応じてデータ主体が利用できるようにすること。但し、商業的な情報が含まれている場合は、当該情報を除去することができます。付録2については、データ主体がデータ輸出者からコピーを取得できない場合には、セキュリティ対策の概要記述と差し替えるものとします。

(h) 準処理を実行する場合、データ輸出者に前もって通知し、データ輸出者から書面による事前の承諾を得ていること。

(i) 準処理者による処理サービスが条項11に従って実施されること。

(j) 条項に基づいて締結した準処理者契約のコピーをデータ輸出者に速やかに送ること。

第6条。 責任

1. 両当事者は、条項3又は条項11に言及された義務の当事者又は準処理者による不履行の結果として損害を被ったデータ主体が、被った損害に対する補償をデータ輸出者から受ける権利を有することに合意します。

2. データ輸出者が事実上消滅するか、法律上存在しなくなるか、又は支払い不能になったため、データ主体が、条項3又は条項11に言及された義務のデータ輸入者又はその準処理者による不履行から生じた損害に対して、第1項に従ってデータ輸出者に対して補償を求める訴えを提起することができない場合、データ輸入者は、データ主体がデータ輸入者に対して、データ輸出者に対する場合と同様に、請求を行うことに同意します。但し、任意の承継法人がデータ輸出者のすべての法的義務を契約又は法律の運用によって承継した場合はこの限りではありません。この場合、データ主体は、当該法人に対して権利を行使することができます。

データ輸入者は、データ輸入者自身の責任を回避するため、準処理者による義務の不履行に依拠することはできません。

3. データ輸出者とデータ輸入者の双方が事実上消滅するか、法律上存在しなくなるか、又は支払い不能になったため、データ主体が、条項3又は条項11に言及された義務の準処理者による不履行から生じた損害に対して、第1項及び2項に従ってデータ輸出者又はデータ輸入者に対して補償を求める訴えを提起することができない場合、準処理者は、データ主体がデータ準処理者に対して、データ輸出者又はデータ輸入者に対する場合と同様に、条項に基づいた自身の処理操作に関する請求を行えることに同意します。但し、任意の承継法人がデータ輸出者又はデータ輸入者のすべての法的義務を契約又は法律の運用によって承継した場合はこの限りではありません。この場合、データ主体は、当該法人に対して権利を行使することができます、 準処理者の責任は、条項に基づく準処理者自身の処理操作に限定されるものとします。

第7条。 調停と裁判管轄

1. データ輸入者は、データ主体がデータ輸入者に対して条項に基づき第三受益者の権利を行使及び/又は損害に対する補償を求めた場合、データ主体の以下の決定を受入れることに同意します。

   (a) 紛争を、独立性を持った人物、又は該当する場合は監督機関による調停に付すこと。

   (b) 紛争を、データ輸出者が設立された加盟国の裁判所に委ねること。

2. 両当事者は、データ主体による選択が、国内法令又は国際法のその他の規定に従って救済を求める、実体的権利又は手続きの権利を害しないことに同意します。

第8条。 監督機関との連携

1. データ輸出者は、監督機関が要求した場合、又は適用されるデータ保護法に基づいて当該供託が必要とされる場合、本契約のコピーを監督機関に預けることに同意します。

2. 両当事者は、監督機関がデータ輸入者、及びすべての準処理者の監査を実施する権利を有することに同意します。この監査は、適用されるデータ保護法に基づいたデータ輸出者の監査に適用される範囲と同じ範囲を有し、同じ条件が課せられます。

3. データ輸入者は、データ輸入者、又は準処理者の第2項に従った監査の実施を阻む、データ輸入者又は準処理者に適用される立法の存在について、データ輸出者に速やかに通知するものとします。 こうした場合、データ輸出者は、条項5 (b)で予見された対策を実行する権利を有するものとします。

第9条。 準拠法

条項は、データ輸出者が設立された加盟国の法律に支配されるものとします。

第10条。 契約のバリエーション

両当事者は、条項にバリエーションをもたせないこと、又は条項を変更しないことを約束します。 これは、両当事者が、条項に矛盾しない限り、必要に応じてビジネス関連問題に関する条項を追加することを妨げるものではありません。

第11条。　準処理

1. データ輸入者は、条項に基づいてデータ輸出者に代わって実施されるいずれの処理操作も、データ輸出者の書面による事前の承諾なしに下請けに出さないものとします。 データ輸入者が、データ輸出者の承諾を得て、条項に基づいた義務の履行を下請けに委ねる場合、データ輸入者は、条項に従ってデータ輸入者に課せられる義務と同じ義務を準処理者に課す、準処理者との書面による契約を通してのみ、それを行うものとします。 準処理者が当該書面契約に基づいてデータ保護義務を果たすことができない場合、データ輸入者は、当該契約に基づく準処理者の義務の遂行について、データ輸出者に対してすべての責任を負うものとします。

2. データ輸出者又はデータ輸入者が事実上消滅するか、法律上存在しなくなるか、又は支払い不能になり、データ輸出者又はデータ輸入者のすべての法的義務を契約又は法律の運用によって承継する承継法人がなかったため、データ主体がデータ輸出者又はデータ輸入者に対して条項6の第1項に言及された補償に対する訴訟を提起できなかった場合、データ輸入者と準処理者間の書面による事前の契約は、条項3で定められている通り、第三受益者条項も提供するものとします。 準処理者の当該第三者責任は、条項に基づく準処理者自身の処理操作に限定されるものとします。

3. 第1項に言及された契約の準処理のデータ保護面に関連する規定は、データ輸出者の設立場所がある加盟国の法律に支配されるものとします。

4. データ輸出者は、条項に基づいて締結され、条項5（j)に従ってデータ輸入者によって通知された準処理契約のリストを保管するものとします。リストは、少なくとも年1回更新されるものとします。 リストは、データ輸出者のデータ保護監督機関が利用できるようにするものとします。

第12条。　個人データ処理サービスの解除後の義務

1. データ輸入者に課せられた法律で移転されたすべて又は一部の個人データの返却又は破壊が禁止されていない限り、両当事者は、データ処理サービスの規定の解除時点で、データ輸入者と準処理者が、データ輸出者の選択に従い、すべての移転された個人データ及び個人データのコピーをデータ輸出者に返却するか、又はすべての個人データを破壊し、破壊した旨をデータ輸出者に証明することに同意します。その場合、データ輸入者は、移転された個人データの秘密保持を確約すること、並びに今後はもう移転された個人データを積極的に処理しないことを保証します。

2. データ輸入者と準処理者は、データ輸出者及び/又は監督機関の要求に応じて、第1項に言及された対策の監査用にデータ処理施設を提示することを保証します。

標準契約条項の付録1

データ輸出者
データ輸出者とは(移転に関連する業務を簡単に記述してください):

お客様とは、SISWによって提供されるクラウドサービスの加入者です。これにより、お客様によって承認されたエンドユーザーが、契約及びクラウドサービスの関連ドキュメントに記載された通りに、お客様データ(個人データが含まれる場合があります)を入力、変更、使用、削除、ダウンロード、或いは処理することが許可されます。

データ輸入者
データ輸入者とは(移転に関連する業務を簡単に記述してください):

Siemens Product Lifecycle Management Software Inc.は、自社及び/又はその準処理者を通して、クラウドサービスを提供します。クラウドサービスには次のものが含まれます。クラウドサービスが運用されている米国及び欧州連合内のコンピューティングインフラストラクチャーの保守、お客様によってクラウドサービスにアップロードされたお客様データのインフラストラクチャー上での保存、クラウドサービスとインフラストラクチャーの可用性及び現在進行中の操作の監視、並びに契約及びクラウドサービスの関連ドキュメントの記載に従ったインフラストラクチャーのセキュリティの保守。

データ主体
移転される個人データは、データ主体の以下のカテゴリーに関係します(記述してください):

データ輸出者によって書面で明示的に指定されていない限り、データ主体には、お客様によってクラウドサービスの使用を承認されたエンドユーザー、及びクラウドサービスに個人データが保存されている他のお客様関係者を含めることができます。

データのカテゴリー
移転される個人データは、データの以下のカテゴリーに関係します(記述してください):

クラウドサービスに保存する特別のデータカテゴリーは、お客様による有意な構成によって決まりますが、クラウドサービスに保存される可能性があるデータの一般的なカテゴリーの一例として、次のものが挙げられます:名前、電子メールアドレス、会社名、電話番号、勤務地、国籍又は市民権、及びクラウドサービスへのアクセス及び使用に関する情報。 お客様のクラウドサービスの構成に応じて、その他の多くのデータカテゴリーがお客様データに存在する可能性があります。

特別カテゴリーのデータ(該当する場合)
移転される個人データは、データの以下の特別カテゴリーに関係します(記述してください):

クラウドサービスに保存する特別データカテゴリーは、契約又は注文での両当事者間の合意に基づくか、或いはクラウドサービスの展開の一部としてお客様に提供するプロフェッショナルサービスの作業明細書の記載に従うことになります。

処理操作
移転される個人データは、以下の基本的な処理業務の対象となります(記述してください):

個人データは、次の方法で処理できます: お客様の構成に応じたクラウドサービスの通常操作の一部としての処理、シングルテナント又はマルチテナント環境でデータ輸出者によって保守されるコンピューティングインフラストラクチャー上での保存及び/又はアーカイブを通した処理、お客様によってクラウドサービスの使用を許可されたエンドユーザーがクラウドサービスに出した指示に従ったアクセス又は送信、並びにデータ輸出者によって実施されるクラウドサービスの保守操作の一部としての処理。

標準契約条項の付録2

一部のクラウドサービス提供は、別の条件に基づいて提供されています。これらの条件は、該当する場合注文に記載されます。 該当しない場合、データ輸入者は、条項の条項4(d)及び5(c)に従って、以下に記載された、システムに保存されている個人データに関する技術的及び組織的な対策を遂行します。

条項4(d)及び5(c)に従ってデータ輸入者によって実施される技術的及び組織的なセキュリティ対策の記述:

1. 物理的アクセス制御。 個人データを処理及び/又は使用するデータ処理システムが設置されている敷地、建物、又は室内への、権限のない人物の物理的なアクセスを防止します。

   対策: すべてのデータセンターは、警備員、監視装置、動作感知装置、アクセス管理機構、並びに装置とデータセンター施設を不正侵入から守るその他の対策によって強化された、厳しいセキュリティ手順を守ります。 権限ある代表者だけが、データセンター施設内のシステム及びインフラストラクチャーにアクセスできます。 正しく機能することを保証するため、物理的セキュリティ装置(運動センサー、カメラ等)の定期的な保守が実施されます。 より詳しく記載すると、以下の物理的セキュリティ対策が、すべてのデータセンターで実装されています。

   a. 通常、建物のセキュリティは、アクセス制御システム(スマートカードアクセスシステム)を通して保護されます。
   b. データセンター施設に物理的にアクセスするため、電子アクセスバッジ(従業員、ベンダー、又は請負人に固有)及びPINを含む許可証明書が、権限が認められた担当者に提供されます。
   c. データセンターのシステム境界内への物理的アクセスは、電子アクセス制御システム(建物に入る際及び入室時はカードリーダーとPINパッド、建物を出る際及び退室時はカードリーダーのみで構成)によってさらに制限されます。
   d. セキュリティ区分に応じて、建物、個々のエリア、及び周囲の敷地が、追加対策によってさらに保護されます。 こうした対策には、特定のアクセスプロファイル、ビデオ監視、侵入警報装置及び生体認証アクセス制御システムがあります。
   e. アクセス権は、以下で定められたシステム及びデータアクセス制御対策に従って、権限が認められた担当者ベースで付与されます。 これは、訪問者のアクセスにも適用されます。 SISWの建物に入る来賓並びに訪問者は、必ず受付で記名しなければならず、訪問には権限が認められたSISW担当者の同行が必要となります。 SISW及びすべての第三者データセンタープロバイダーは、データセンター内のSISWのプライベートエリアに入った人物の名前と時間を記録します。
   f. SISWの従業員及び外部関係者は、SISWのあらゆる場所で各自IDカードを着用する必要があります。

2. システムアクセス制御。 クラウドサービスの提供に使用されるデータ処理システムは、許可なく使用されないようにする必要があります。

   対策:

   a. SISW又はその準処理者は、NIST SP 800-53 Rev 4 Access Control(アクセス制御)(AC)及びIdentification and Authentication(識別および認証)(IA)の要件に従って環境を管理します。
   b. 個人データの保存と処理を実行するシステムを含めた、機密性が高いシステムへのアクセスを許可するには、複数の権限レベルが使用されます。 認定ユーザーのみがユーザーの追加、削除、又は変更に対する適切な権限を持つようにするため、複数のプロセスが設けられています。
   c. すべてのユーザーは、一意のユーザー名と、特定の複雑さの最小条件に合致する必要があるパスワードを使用して、SISWのシステムにアクセスします。
   d. SISWとその準処理者は、要求された権限変更がガイドラインに従ってのみ実行されることを保証するため、手順を規定しています(許可なく権利が付与されないこと等)。 SISWユーザーが役割を変えた場合、或いは会社を辞めた場合、環境へのアクセス権を取消すプロセスが実施されます。
   e. SISWと準処理者は、パスワードの共有の禁止、パスワードが開示された場合に必要な措置、すべてのユーザーパスワードの定期的な変更の実施、デフォルトパスワードの変更の実施を定めた、パスワードポリシーを策定しています。 認証の際、パーソナライズされたユーザーIDが割当てられます。 す

べてのパスワードは、複雑さの最小要件に適合する必要があり、暗号化された形式で保存されています。 ドメインパスワードの場合、システムは、複雑さの最小要件に従って、60日ごとのパスワードの変更を強制します。 各SISWコンピューターには、パスワード保護されたスクリーンセーバーがあります。

f. SISW又はその準処理者は、次のアカウントイベントを自動的に監査します: 作成、変更、有効化、無効化、及び削除。 システム管理者は、ログを定期的に確認します。
g. SISWとその準処理者のネットワークは、ファイアウォールによって公衆インターネットから保護されています。
h. SISWとその準処理者は、企業ネットワークへのアクセスポイント、電子メールアカウント、及びすべてのファイルサーバーとすべてのワークステーションで、最新のウイルス対策ソフトウェアを使用します。
i. SISWとその準処理者は、関連セキュリティアップデートを確実に展開するため、セキュリティパッチ管理を実装します。
j. SISWの企業ネットワーク及びクリティカルなインフラストラクチャーへのフルリモートアクセスは、強力な、多元的認証によって保護されています。

3. データアクセス制御。 データ処理システムを使用する権利を有する担当者は、アクセス権を持つ個人データにのみアクセスします。処理、使用、及び保存の過程で、許可なく個人データの読取り、複製、変更、又は削除を行ってはなりません。

対策:

a. 個人情報、機密情報、又は極秘情報へのアクセスは、必要最小限のベースで付与されています。 すなわち、従業員又は外部第三者は、作業を完了するために必要な情報へのアクセス権を有します。 SISWは、権限の割当て方、及び割当てる権限を文書化した、権限概念書を使用します。 すべての個人データ、機密データ、又は本来であれば慎重に扱うべきデータは、SISWのセキュリティポリシーと基準に従って保護されています。
b. SISWクラウドサービスのすべてのプロダクションサーバーは、関連データセンターで運用されています。 アプリケーション処理担当者、機密情報、又はその他の機密性の高い情報を保護するセキュリティ対策に対して、定期的なチェックが行われています。 そのために、SISWは定期的な外部監査も組込んで、これらの対策が適切な方法で適用されていることを確認しています。
c. SISWは、SISWによって承認されていない個人ソフトウェア又はその他のソフトウェアを、クラウドサービスに使用するシステムにインストールすることを許可しません。
d. 基礎のデータストレージ媒体の障害により、データを移転する必要が生じた場合、当該移転の完了時に、障害のあるストレージ媒体は、消磁されるか(磁気ストレージの場合)又は細断されます(ソリッドステート又は光学式ストレージの場合)。

4. データ送信制御。 移転中に個人データの読取り、複製、変更、又は削除が許可なく行われないようにする必要があります。

対策:

a. SISW又はその準処理者は、NIST SP 800-53 Rev 4 Systems and Communication Protection(システムおよび通信の保護)(SC)の要件に従って、インフラストラクチャー及び構成を管理します。 これには、インフラストラクチャーの外部境界で悪意のある通信を防ぐため、システム境界に配置されたネットワークベースの侵入防止システム(NIPS)とファイアウォールが含まれます。 NIPSとファイアウォールは、DISA STIG規格に従って構成されています。 データは、FIPS 140-2に準拠する暗号モジュールを使用して、送信中に暗号化されます。
b. データ記憶媒体が物理的に輸送される場合、同意したサービスレベルを保証するため、SISWで適切な対策が実施されます(暗号化、及びリード線付きの容器等)。
c. SISWの内部ネットワークを介した個人データの送信は、SISWのセキュリティポリシーに従ってその他の機密データを送信するときと同じ方法で保護されます。
d. データがSISWとお客様の間で移転されるとき、移転される個人データの保護対策は、契約又はクラウドサービスの関連ドキュメントの規定に基づきます。 これは、物理ベースとネットワークベースの

両方のデータ移転に適用されます。 お客様は、SISWの境目(例えば、クラウドサービスをホストするデータセンターの送信元のファイアウォール)からのデータ移転に対する責任を負います。

5. データ入力制御。 クラウドサービスは、クラウドサービスの提供に使用するインフラストラクチャーにおける個人データの入力、変更、又は削除の実行の有無、及び実行者を、過去に遡って判断することを許可します。

対策:

a. SISWは、作業を進める過程で必要に応じて、権限が認められた担当者にのみ個人データへのアクセスを許可します。 SISWは、SISW又はその準処理者による個人データの入力、変更、及び削除、又は遮断をログに記録するシステムを、クラウドサービスでサポートされる最大限度まで実装しました。
b. 監査証跡は、不正な動作又は誤動作が発生したか、発生が疑われる場合、イベントの再構築を容易にするために必要な、十分な詳細を提供します。 各オペレーティングシステムのイベントログレコードには、イベントタイプ、タイムスタンプ、イベントの発生源、イベント発生場所、イベントの結果、及びイベントに関連するユーザーが含まれます。

6. ジョブ制御。 個人データは、契約の条件及びお客様からの関連指示に従ってのみ処理されます。

対策:

a. SISWは、SISWとお客様、準処理者、又はその他のサービスプロバイダー間の契約の順守を保証するため、制御とプロセスを使用します。
b. お客様データには、SISW Information Classification (SISW情報分類)規格に従った機密情報と、同じ保護レベル以上のレベルが適用されます。
c. SISWのすべての従業員及び契約パートナーは、SISWのお客様及びパートナーの営業秘密を含むすべての極秘情報の秘密保持義務を遵守するため、契約による拘束を受けます。

7. 可用性制御。 個人データが、偶発的又は不正な破壊又は損失に対して保護されます。

対策:

a. SISWは、必要時にビジネスクリティカルなシステムの迅速な復元を保証する、バックアッププロセス及びその他の対策を採用しています。
b. SISWは、データセンターへのパワー供給を確実なものとするため、グローバルなクラウドサービスプロバイダーに依拠しています。
c. SISWは、クラウドサービス向けの危機管理計画、並びに業績及び障害回復戦略を定義しています。

8. データ分離制御。 別の目的で収集された個人データを個別に処理することができます。

対策:

a. 該当する場合、SISWは、展開されたソフトウェアの技術機能(例: マルチテナンシー又はシステムランドスケープの分離)を使用して、お客様の個人データを他のお客様の個人データから分離します。
b. SISWは、お客様ごとの専用インスタンスを(論理的又は物理的な分離によって)維持します。
c. お客様(お客様の関連会社を含む)は、お客様自身のお客様インスタンスへのアクセス権のみを有します。

9. データ完全性制御。 処理業務中に個人データが、元のままの、完全、且つ最新の状態に保たれていることを保証します。

対策: SISWは、不正な変更からの防御として、防衛戦略を複数のレイヤーに実装しています。 これは、上記の通り、制御及び対策の条で定められた制御を指します。 ファイアウォールの設定により、パブリックアクセスとプライベートアクセスを分離する、複数のネットワークセグメントを実現します。 各ファイアウォールルールセットには、これらのセグメント間で許可される通信を指定する、特定のアクセス制御があります。

a. セキュリティ監視センター: 警告、調査、及び必要に応じて通知並びにセキュリティインシデントの改善支援を行うため、自動侵入検知ソフトウェアをその他のセキュリティ防御及びフォレンジック調査ソフトウェア並びにプロセスと共に使用します。
b. ウイルス対策ソフトウェア: ウイルス、ワーム、トロイの木馬、及びその他の形式のマルウェアを防ぐため、すべてのシステムに最新のウイルス対策定義が設定されます。
c. バックアップとリカバリ: すべてのシステムにデータと設定の基本レベルのバックアップスナップショットがあります。　該当する場合、SISWとその準処理者は、さらに、互いの距離が十分離れた2か所のデータセンターにデータを保存する、高可用性構成でお客様のインスタンスを運用します。
d. セキュリティ対策の妥当性を証明するための定期的な外部監査。　SISWとその準処理者は、上記のセキュリティ対策をテストするため、定期的な外部監査を実施します。