

## 調達契約条件

**1. 契約の基礎的な内容:** ここに記載されている調達契約条件、表紙、取引条件、管理に関する詳細、添付資料をすべてまとめたものを「発注契約」と総称します。この発注契約により、商品、サービス、ソフトウェアライセンス、この発注契約に記載されているその他の該当物（「製品」と総称します。これらを個別に言及する場合も「製品」と記載します）を NortonLifeLock Inc. とその関連企業（これ以降は「NLL」と表記）が購入するための条件が規定されます。NLL による購入には、必ずこの発注契約条件が適用されることとします。この発注契約の対象者は、販売者、サプライヤー、製品の供給者（これ以降は「サプライヤー」と総称）です。サプライヤーは、製品を出荷するか、製品の出荷を約束することにより、NLL の購入条件に同意したことになります。また、この発注契約に同意した場合や、この発注契約に従って行動した場合も、NLL の購入条件に同意したことになります。

NLL の購入条件に対する同意は、この発注契約に記載されている条件によって明示的に制限されることとします。NLL は、サプライヤーが提案するすべての条件を完全に拒否する権限を有しています。これらの条件には、見積書に記載された条件、請求書に記載された条件、この発注契約に記載されている条件とは異なる条件（または追加された条件）などがありますが、これらだけに限定されるものではありません。サプライヤーは、これらの異なる条件や追加条件がこの発注契約の締結日の前に規定されたのか後に規定されたのかに関係なく、これらの条件が NLL とサプライヤーによって拒否される場合があることに同意するものとします。また、適切な権限を持つ NLL の代表者と関係者との間で個別の合意を得ない限り、これらの条件は無効な条件とみなされるということに同意するものとします。

**譲渡の禁止:** NLL もサプライヤーも、相手から書面による同意を事前に得ることなく、法の施行や所有権の変更などにより、すべてであるか一部であるかにかかわらず、この発注契約または個別の権利と義務を他者に譲渡することはできません。ただし、合併、買収、資産の売却、資産の譲渡などの方法で後継企業に譲渡する場合や、譲渡先事業体の共通の管理下にある（または譲渡先事業体を管理する）事業体に譲渡する場合を除きます。ただし、その場合も、サプライヤーは NLL の競合他社に譲渡することはできないという条件が適用されます。

**コンプライアンス:** この発注契約で規定されている NLL のコンプライアンスに関する不明点（使用制限や使用量のコンプライアンスに関する不明点など。ただし、これらだけに限定されるものではありません）については、NLL とサプライヤーで誠実な話し合いを行うこととします。サプライヤーは、NLL の回答が正確ではない（または不十分である）という確証がある場合、NLL の使用記録が業界標準に準拠しているかどうか、個別の秘密保持契約の同意事項に準拠しているかどうかについての評価を、信頼できる中立的な第三者の監査人に依頼することができます。こうした依頼を受けた第三者は、調査結果に基づく補償を受けることができない場合があります。

## 2. 支払いと請求:

- A. **価格:** この発注契約に記載されている価格は、NLL が製品に対して支払う最大の金額であり、すべての費用、配送料、梱包料、取り扱い料、配送時の保険料が含まれた金額です。
- B. **支払い:** この発注契約で特に明記されていない限り、NLL が請求書または製品を受領してから 60 日以内に、この発注契約で規定された金額を異議なく支払うこととします。
- C. **費用:** 費用は、NLL が規定するサプライヤーの出張経費に関するポリシーに従い、この発注契約で規定された費用を超えない金額で、マークアップを除いた実費で払い戻されることとします。
- D. **税:** この発注契約に記載されている価格には、連邦税、州税、地方税は一切含まれていません。適用されるすべての税額は、サプライヤーの請求書に別途記載されるものとします。NLL の購入に関連して源泉徴収税が発生する場合、NLL はその税額を本契約に基づく金額から差し引き（税額を差し引いた金額が全支払額になります）、サプライヤーの要求に応じて、税額控除を申請するための証明文書を提供することとします。
- E. **請求:** (i) すべての請求書で、各明細行に発注項目の行番号と、数量、単価、単位を記載する必要があります（該当する場合は、出荷地点、詳細な配送ルート、前払いの配送料も記載）。この形式に従っていない請求書は拒否されることとします。(ii) すべての請求書の締日は、製品、サービス、ソフトウェアライセンス、その他の該当物が納品された（または使用可能になった）月の翌月末になります。請求額には、払い戻し可能な発生費用が含まれます（たとえば、10 月に発生した手数料や費用は、11 月 30 日までに請求する必要があります）。(iii) 本契約で規定されている金額についてのみ、期日までに支払いを行うことに双方が合意することとします。本段落に明記されていない金額の請求や支払いを行うことはできません。サプライヤーとその代表者は、こうした金額を請求するための一切の権利を放棄することとします。適用される他の条件と矛盾する場合は、本段落の条件が優先されます。他の条件を本段落の条件よりも優先させることはできません。

## 3. 製品の受け渡し:

 特に明記されていない限り、以下の条件が適用されることとします。

- A. NLL が指定する受け渡し場所で実際に製品が納品された時点で、その製品の所有権が NLL に移り、製品の損失や損害のリスクも NLL が負うこととなります。サプライヤーは、NLL の社員の不正行為や過失が原因である場合を除き、NLL が拒否した製品の損失や損害のリスクを負うものとします。
- B. NLL は、追加料金を支払うことなく、製品のすべてまたは一部について、納品のスケジュールをいつでも変更することができます。その場合、NLL が指定した新しい配達日が納品予定日になります。

- C. すべての製品は、以下の方法で梱包することとします。(i) 適切な商習慣に準拠した方法であること。(ii) 特定の製品を最低料金で配送する場合に、一般的な運送業者に受け入れられる方法であること。(iii) I.C.C. 規制に準拠した方法であること。(iv) 指定された配送場所に製品を安全に配送できる方法であること。
- D. すべてのコンテナに、NLL が指定する出荷情報(発注番号、カートン数、サプライヤーのパーツ番号、その他固有のマーキングなど)とコンテナの取り扱い方法が記載されたラベルなどを貼る必要があります。
- E. すべての配送製品は、部分的または完全な製品として取り扱う必要があります。また、NLL の名前、受取人の氏名、詳細な配送先住所(建物名を明記)、発注番号、数量、配送に関する注記、配送コンテナの寸法、正味重量、総重量が記載されたパッキングリストをすべての配送製品に添付する必要があります。
- F. 過剰配送があった場合、NLL は、着払いで返品することができます。その際の費用は、サプライヤーが負担するものとします。
- G. 納品予定日より前に製品が配送された場合、NLL は、(1) サプライヤーが着払い費用を負担する形で製品を返却することも、(ii) 実際に NLL が製品を受領した日付ではなく、元の納品予定日に基づいた支払いを行い、その製品を受領することもできます。
- H. 事前の検査や支払いに関係なく、すべての製品は、受領後の妥当な期間内に、NLL の施設で最終的な検査を受けることとします。この最終検査により、製品を受け入れるか返品するかが決定します。
- I. サプライヤーは、返品されたすべての配送製品の記録を残す必要があります。サプライヤーは、返品された製品の輸出や輸入について該当国で規定されているすべての規制を順守する必要があります。

**4. 保証と救済措置:** サプライヤーは、サプライヤーとその担当者が以下の条件に従うことを NLL に対してここに表明し、保証することとします。

- A. 本契約を履行するために必要なすべての権限、ライセンス、許可、同意、法的文書を有し、該当するすべての法律、規約、規制(データのプライバシー、輸出入、環境、危険物などに関する法律、規約、規制。ただし、これらだけに限定されるものではない)に完全に準拠する。
- B. 本契約に関する実際の利益相反や潜在的な利益相反について知ることはなく、本契約の履行によって第三者との合意に違反することはない。
- C. 第三者が所有する機密情報や資料について、サプライヤーがそれらの情報や資料を使用するための許可を第三者から書面で得ない限り、サプライヤーがそれらの情報や資料を使用することはない、NLL に提供することもない。
- D. 業界の基準に準拠した専門的な方法で、必要な注意を払い、スキルと勤勉さをもって、本契約を履行する。
- E. 製品は、使用されたものや再生されたものとして明示的に購入していない限り、新品を提供する。
- F. 本契約で規定されている仕様を満たす製品を提供する。または、双方が書面で明示的に合意した仕様を満たす製品を提供する。
- G. 特定の製品が第三者の知的財産権を侵害しているというクレームが、サプライヤー(またはサプライヤーの供給元)に対して申し立てられることがないようにする。
- H. 何らかの媒体を介して製品を NLL に配送する場合、その媒体の素材や仕上がりに欠陥がないようにする。
- I. ソフトウェアや技術製品を納品する場合は、ウイルスや不正なコードが含まれていない製品を納品する。また、商業的に妥当な手段で製品の検査を行い、ウイルスや不正なコードを検出して完全に削除し、製品にウイルスや不正なコードが含まれていないことを確認した上で、製品を納品する。

項目番号 4.E、4.F、4.H のいずれか(またはこれらすべて)で規定されている保証条件に違反した場合、サプライヤーはただちに費用を全額負担することとします。また、NLL は次の権利を有しています。(i) NLL が妥当なレベルで満足できる製品の再納品を要求する。(ii) 欠陥のある製品に対して支払った料金や、本契約に準拠した製品をサプライヤーが納品できなかったために、その製品を使用して NLL に損害が発生した場合に、その製品に対して支払った料金の払い戻しを要求する(その場合、サプライヤーは、本契約の「取り消し」条項の規定に従い、NLL が追加の通知を行うことなく本契約のすべてをキャンセルできることに同意するものとする)。

本契約で規定されている場合を除き、サプライヤーは、特定の使用目的に関する商品性や適合性などについて(ただし、これらだけに限定されるものではありません)、明示的であるか暗黙的であるかを問わず、上記以外のいかなる保証も行わないこととします。

**5. 契約の終了:**

NLL が本契約に対する重大な違反を犯し、その違反が詳述された書面をサプライヤーから受け取ってから 30 日以内にその違反を是正しなかった場合(または、違反を是正するための妥当な計画を提示しなかった場合)、サプライヤーは本契約を終了することができます。NLL は、書面でサプライヤーに通知することにより、原因の有無を問わず、いつでも本契約を終了することができます(すべて終了することも、部分的に終了することもできます)。契約終了通知に明記されていない限り、契約の終了は即時に有効になります。

こうした契約終了の場合、サプライヤーが NLL に請求できる唯一の補償は、契約の終了前に NLL が実際に受領して承認した製品の価格に相当する金額だけです。サプライヤーは、これ以外の金額を受領したり収集したりする権利を放棄することとします。サプライヤーの不履行によって本契約が取り消された場合、NLL は、NLL が妥当であると判断した方法で、取り消された製品に類似した製品をサプライヤーの費用負担で調達できることとします。

6. **免責事項:** サプライヤーは、以下に起因する損失、責任、損害、要求、訴訟、訴訟原因、判決、費用 (裁判費用と合理的な法的費用を含む) について、NLL の役員、管理職、一般社員に対する保護と補償を行うこととします。
- A. サプライヤーまたはサプライヤーと契約している第三者の行為や不作為に起因する物的な損害、人体への傷害、死亡。
  - B. 本契約に基づいてサプライヤーまたはサプライヤーの代理者が準備または提供した製品が、第三者の知的所有権を侵害している (または第三者の知的所有権が不正に使用されている) というクレーム。
  - C. 次に示す根拠により、NLL とサプライヤー (またはサプライヤーの担当者) との間に独立した請負業者以外の関係が存在するというクレームや判断。(a) 英国の場合: 事業譲渡 (雇用保護) 規則 2006。(b) 欧州連合加盟国の場合: 既得権益指令に準拠する国内法。(c) 欧州連合に加盟していない国の場合: 既得権益指令の条項に類似した国または地方の規制。
  - D. 機密データや個人データの保護義務に対する違反 (NLL が保有する機密情報の不正な使用、不正なアクセス、不正な開示など。ただし、これらだけに限定されるものではない) に起因する第三者によるクレーム。

NLL は、NLL に対する要求や、NLL が被告となっている訴訟や訴訟原因を弁護する弁護士を承認する権利を有しています。また、こうした承認が不当な理由で妨げられることがないものとします。サプライヤーは、NLL に関する問題に対する要求、訴訟、訴訟原因の弁護に参加する権利を NLL が有していることに同意するものとします。サプライヤーは、書面による同意を NLL から得ることなく (書面による同意が不当に妨げられることはないものとします) 和解を締結することはできません。ただし、和解によって次の状況が発生する場合を除きます。(i) すべてのクレームから NLL が免除される場合。(ii) 条件に違反している製品 (そうした製品が存在する場合) の使用を停止する以外には、NLL には一切の義務が課されない場合。(iii) NLL または NLL の代理者に対していかなる費用負担も発生しない場合。NLL とサプライヤーの利益で矛盾が発生していると NLL が合理的に判断した場合、NLL は専任の弁護士を指名することができます。

7. **責任の制限:** 死亡、人体に対する傷害、機密保持違反、個人データ保護違反、法規違反、詐欺行為、意図的な不正行為を除き、NLL とサプライヤーは、本契約の条件と、本契約で規定されている製品やサービスについて、間接的な損害、偶発的な損害、特殊な損害、結果的な損害を他の当事者や第三者に対して負うことはないものとします。これらの損害には、訴訟、契約、不法行為に関わらず、いずれかの当事者が被った利益の損失に対する損害が含まれます。いずれかの当事者がそうした損害の可能性について知らされていたとしても、この条件が適用されます。

## 8. 保険:

- A. 双方が署名した個別の同意書類 (本契約で規定されている製品の購入や販売を管理するための同意書類) に明記されていない限り、サプライヤーは、北米、南米、欧州、中東、アフリカに拠点を置く NLL または NLL 関連企業に対し、本契約で規定されている製品とその性能について、以下に示す条件の保険 (米国以外の地域に拠点を置くサプライヤーについては、米ドルでの金額に相当する補償額が規定されている保険) に加入することとします。

- (i) 人身傷害事故、死亡事故、広範囲にわたる物損事故を補償する企業総合賠償責任保険 (契約上の賠償を含む) - 1 回の事故につき最高補償額が 100 万ドル (\$1,000,000) 以上、人身傷害事故と物損事故が同時に発生した場合の最高補償額が 200 万ドル (\$2,000,000) 以上であること。
- (ii) すべての所有車両、非所有車両、レンタル車両を対象とする自動車賠償責任保険 - 1 回の人身傷害事故または物損事故につき、最高補償額が 100 万ドル (\$1,000,000) 以上であること。
- (iii) 傷害、疾病、死亡に対する雇用者の賠償責任補償が含まれている労働者補償保険 (該当地域の法律によって規定されている場合) - 1 回の事故と社員 1 人につき、最高補償額が 100 万ドル (\$1,000,000) 以上であること。
- (iv) 企業包括賠償責任保険 - 1 回の賠償案件につき、最高合計補償額が 300 万ドル (\$3,000,000) 以上であること。
- (v) 専門職業人賠償責任保険 (E&O 保険) - クレームフォーム 1 件につき、年間合計の最高補償額が 200 万ドル (\$2,000,000) 以上であること。

A.M. Best Company による信用格付けが A-1 以上の保険会社が提供する保険に加入する必要があります。本契約を発行する NLL 事業体は、被保険者として企業総合賠償責任保険証券に追加されることとなります。NLL の保険証券で規定されている補償内容を適用する権限がない場合は、保険会社が発行する企業総合賠償責任保険証券が一次保険となります。保険証券には、利害の分離条項が記載されていることとします。取り消しを行う場合は、取り消しの 30 日前までに書面で通知する必要があります。支払いを行わない場合は、10 日前までに通知する必要があります。

いかなる場合においても、前述の補償範囲の制限により、サプライヤーの契約上の補償責任が影響を受けることはありません。サプライヤーが請負業者と契約している場合、サプライヤー自身の責任において、本条項に記載されている条件を満たす保険に請負業者を加入させる必要があります。本契約に基づくサプライヤーの行動は、すべてサプライヤー自身の責任において行われることとし、サプライヤーの社員や代理店は、NLL が加入している保険による補償等は一切受けられないこととします。

- B. オーストラリアに拠点を置く NLL の場合、本契約で規定されている製品とその性能について、サプライヤーは、オーストラリアの法律で義務付けられている保険などのサービス (自動車賠償責任保険、労働災害保険、提供するサービスや製品に適した一般的な事業保険など) の契約を信頼できる保険会社と結び、本契約の有効期間中はその効力を維持するものとします。たとえば、以下の補償内容が定義されている保険を契約する必要がありますが、これらだけに限定されるものではありません。

ません (最高補償額が米ドル以外の通貨で規定されている場合は、米ドルでの金額に相当する補償額が規定されている保険を契約する必要があります)。

- (i) 一般賠償責任および製造物賠償責任保険 - 最高賠償額が 10,000,000 オーストラリアドル以上であること。また、NLL にとって有利な条件の免責事項が保険証券に記載されていること。
- (ii) サプライヤーまたはサプライヤーに代わって作業を行う請負業者による過失や不作為に起因する損害を補償するための専門職業人賠償責任保険または IT 賠償責任保険 - 最高賠償額が 1,000,000 オーストラリアドル以上であること。

NLL の保険証券で規定されている補償内容を適用する権限がない場合は、サプライヤーが契約する保険が一次保険とみなされます。いかなる場合においても、前述の補償範囲の制限により、サプライヤーの契約上の補償責任が影響を受けることはありません。サプライヤーが請負業者と契約している場合、サプライヤー自身の責任において、本条項に記載されている条件を満たす保険に請負業者を加入させる必要があります。本契約に基づくサプライヤーの行動は、すべてサプライヤー自身の責任において行われることとし、サプライヤーの社員や代理店は、NLL が加入している保険による補償等は一切受けることができないこととします。

- C. インドに拠点を置く NLL の場合、本契約で規定されている製品とその性能について、サプライヤーは、インドの法律で義務付けられている保険 (自動車賠償責任保険や、提供するサービスや製品に適した一般的な事業保険など) の契約を信頼できる保険会社と結び、本契約の有効期間中はその効力を維持するものとします。たとえば、以下の補償内容が定義されている保険を契約する必要がありますが、これらだけに限定されるものではありません (最高補償額が米ドル以外の通貨で規定されている場合は、米ドルでの金額に相当する補償額が規定されている保険を契約する必要があります)。

- 1) 契約上の賠償責任、人身傷害、広告による損害などを補償するための一般賠償責任保険 - 最高賠償額が現地通貨換算で 1,000,000 米ドル相当以上であること。
- 2) サプライヤーまたはサプライヤーに代わって作業を行う請負業者による過失や不作為に起因する損害を補償するための E&O 保険 - 最高賠償額が現地通貨換算で 1,000,000 米ドル相当以上であること。

本契約を発行する NLL 事業体は、被保険者として保険証券に追加されることとなります。

NLL の保険証券で規定されている補償内容を適用する権限がない場合は、サプライヤーが契約する保険が一次保険とみなされます。いかなる場合においても、前述の補償範囲の制限により、サプライヤーの契約上の補償責任が影響を受けることはありません。サプライヤーが請負業者と契約している場合、サプライヤー自身の責任において、本条項に記載されている条件を満たす保険に請負業者を加入させる必要があります。本契約に基づくサプライヤーの行動は、すべてサプライヤー自身の責任において行われることとし、サプライヤーの社員や代理店は、NLL が加入している保険による補償等は一切受けることができないこととします。

## 9. 当事者と担当者との関係

- A. サプライヤーは、本契約の条件 (機密情報や個人データの保護に関する条件など。ただし、これらだけに限定されるものではありません) を順守するための書面による合意を、自社の社員、請負業者、下請業者、代理店、サプライヤーまたはサプライヤーの代理者と契約している第三者 (「担当者」と総称します。これらを個別に言及する場合も「担当者」と表記します) と結ぶこととします。関連する作業指示書のすべての要件が、担当者に適用されます。また、サプライヤーは、サプライヤーの担当者によるすべての行為、不作為、違反について、サプライヤー自身がそうした行為を行った場合と同様に、NLL に対してすべての責任を負うこととします。
- B. サプライヤーは、NLL にとって常に独立した請負業者であるとみなされます。本契約のいかなる条件も、サプライヤーと NLL との間で、パートナーシップ、合併事業、共同雇用、雇用、フランチャイズ展開、代理店経営などを行うことを意図したものではなく、そのように解釈することもできないものとします。両当事者 (サプライヤーと NLL) は、明示的であるか暗黙的であるかにかかわらず、一方の当事者に代わって、義務を負ったり、義務を発生させたりする権限を有していると表明することはできません。サプライヤーは独立した請負業者として、製品を提供するための手段と方法を決定する責任を単独で負うものとします。また、サプライヤーは、(a) 連邦、州、地方で規定されているすべての法律や規制などに従い、該当するすべての支払い、報告、徴収 (連邦、州、地方の税金、社会保障、失業補償、寄付、源泉徴収など。ただし、これらだけに限定されるものではありません) を担当者に対して行う責任と、(b) 該当するすべての賃金、福利厚生、その他の報酬を担当者に支払う責任があります (医療、歯科、労働者の補償、障害保険、年金、退職金など。ただし、これらだけに限定されるものではありません)。これらの条件は、NLL には適用されません。
- C. 本条項に記載されている条件は、次のいずれかの条件を満たすサプライヤー担当者にのみ適用されます。(i) NLL が指定する場所でサービスを提供する担当者。(ii) 個人データにアクセスする担当者。(iii) NLL の顧客の機密情報にアクセスする担当者。(iv) NLL が所有または使用するネットワーク、システム、またはデータレポジトリにアクセスする担当者 (「指定サービス」と総称。これらを個別に言及する場合も「指定サービス」と表記します)。上記の条件を満たすサプライヤー担当者は、NLL

が規定する作業規則、ポリシー、作業手順を順守する必要があります。NLL の明示的な同意を得ることなく、NLL の施設にある資料、データ、資産を削除することはできません。NLL から配置換えの要求があった場合、サプライヤーは、指定サービスを行うために割り当てられた関係者を担当から外し、同等以上のスキルを持つ関係者を代わりに配置する必要があります。NLL は、こうした配置換えに伴って発生するトレーニングや研修にかかる時間と費用を負担することはないものとします。サプライヤー担当者が指定サービスを実行する前に、サプライヤーは次の条件を保証することとします。(a) 現地の法律で許可されている範囲内で、SOW、本契約書の添付資料、当事者間で合意した書類に従い、関係者について必要な背景調査を実施する(その際、調査を実施するための許可を得ること)。調査内容が明確に定義されていない場合は、関係者ごとに、地方、郡、連邦の背景調査を行い、身元情報、学歴、就労資格、不正行為による有罪判決の有無(詐欺、窃盗、横領など。ただし、これらだけに限定されるものではない)、他社に対する傷害行為や傷害の虞の有無などを調べる。(b) こうした背景調査で、サービスの実施に悪影響を与えるような情報が見つからなかった場合、(c) サプライヤーは、本条項に記載されている条件に従い、背景調査の結果または証明書(あるいはその両方)を NLL に提出する(NLL は、これらの書類の提出を随時要求する場合があります)。NLL は、法的な根拠に基づき、NLL の施設やネットワークへのアクセスをいつでも拒否できる権限を有しています。本条項に記載されている条件にサプライヤーが違反した場合、本契約に対する重大な違反とみなされます。

- 10. 成果物と所有権:** 本契約に従って NLL に提供された(または NLL 用に準備された)すべての有形物、無形物、ハードウェア、機器、ドキュメント、書類、データ、コンテンツ、グラフィックデザイン、写真、レポート、ワークフロー、ソフトウェア(アップデートとドキュメントを含む)、フィードバック、その他の資料、ソフトウェア製品(NLL のオンプレミス環境に導入されているソフトウェア、サプライヤーの環境に導入されているソフトウェア、クラウド環境のソフトウェア、プロバイダ環境のソフトウェア、サブスクリプション契約のソフトウェア、SaaS 契約のソフトウェア、その他のソフトウェアサービスのすべてが対象になります)で入力、処理、生成、出力されたデータと情報(「サービスの結果」)は、NLL の独占的資産になります(ただし、これらだけに限定されるものではありません)。サプライヤーは、該当する法律で許可される最大限の範囲内で、サービスの結果に対する権利、所有権、利益が NLL の独占的所有物であることに同意するものとします。これらの権利には、すべての著作権、特許権、トレードシークレット、商標、知的財産権(「IPR」と総称。これらを個別に言及する場合も「IPR」と表記します)などが含まれますが、これらだけに限定されるものではありません。サービスの結果に対するすべての権利、所有権、利益が NLL の独占的所有物ではない場合、サプライヤーは、サービスの結果に対するすべての権利、所有権、利益と、すべての IPR(アプリケーション、拡張機能、アップデートなど。ただし、これらだけに限定されるものではありません)を完全に NLL に譲渡することに同意するものとします。NLL から要求があった場合、サプライヤーは、該当する権利を NLL に譲渡することに同意する書類と、NLL がサービスの結果で IPR の導入、保存、補完を行うために必要なドキュメントを提出することに同意するものとします。サプライヤーは、サービスの結果においてサプライヤーが持ち得るすべての「道徳的権利」を放棄して NLL に譲渡し、道徳的権利を主張しないことに同意するものとします。サービスの結果に対する権利を NLL に譲渡できない場合、サプライヤーは、サービスの結果とすべての IPR について、非限定的で永続的で全世界的な全額支払済みの取消不能ライセンスを NLL に譲渡することに同意するものとします。これらの権利には、サービスの結果の派生物の使用権、複製権、販売権、配布権(直接配布する権利と、複数のチャネルを経由して配布する権利を含む)、作成権、所有権が含まれますが、これらだけに限定されるものではありません。こうした譲渡について、NLL はサプライヤーに説明する責任を負うことはないものとします。

本契約に従い、サプライヤーが所有している(またはライセンスを取得している)既存の成果物を NLL に提供する場合(またはサービスの結果に組み込む場合)、サプライヤーは、サービスの結果に対する NLL のすべての権利を NLL が行使するために必要な範囲内において、その既存の成果物とすべての IPR に対する非限定的で永続的で全世界的な全額支払済みの取消不能ライセンスを NLL に譲渡することに同意するものとします。「既存の成果物」とは、本契約に基づいてサプライヤーまたはサプライヤーの代理者が事前に作成したすべての製品、情報、資料のことを指します。既存の成果物には、デザイン、発明、オブジェクトコード、ソースコード、ドキュメント、メソッド、仕様書、資料、ツールなどが含まれますが、これらだけに限定されるものではありません。

## 11. 機密情報

「機密情報」とは、(i) すべての個人データ、(ii) いずれかの当事者がもう一方の当事者に提供または開示したすべての非公開情報(この行為を「開示」と呼び、情報の開示を受ける当事者のことを「受領者」と呼びます)、または本契約を履行する過程においていずれかの当事者から取得した情報のことを指します。これらの情報には、ソフトウェア、プログラム、価格、プロセス、要件、ドキュメント、銀行口座、クレジットカード、財務計画、マーケティングプラン、ビジネスプランに関する情報、情報開示の際に機密情報や占有情報として判断された資料や情報、妥当な理由により機密情報または占有情報として判断される情報などが含まれますが、これらだけに限定されるものではありません。「個人データ」とは、特定の自然人(「データ主体」)を識別するための情報のことを指します。この場合の「自然人」とは、氏名、識別番号、場所データ、オンライン ID などの情報によって直接的または間接的に特定できる個人、または、肉体的、生理的、遺伝的、精神的、経済的、文化的、社会的な側面において、1 つ以上の要素によって直接的または間接的に特定できる個人のことです。この「データ主体」は、NLL (または NLL の代理店やディストリビュータ)の社員、請負業者、エンドユーザー、顧客、顧客のエンドユーザー、顧客の社員、その他の第三者を指す場合があります。明確に定義すると、すべてのサービスの結果と、NLL または NLL の代理店が製品にアップロードしたすべての情報、データ、コンテンツが、NLL の機密情報というこ

とになります。個人データを除き、次に示す情報には受領者の機密保持義務は適用されません。(a) 受領者が過失や違反を行うことなく公開した情報、(b) 機密保持の義務を負うことなく受領者に提供された情報(第三者から直接提供された情報と、第三者から正当な方法で提供された情報を含む)、(c) 開示者の機密情報を使用したり参照したりすることなく、受領者が独自に作成した情報、(d) 書面による開示者の承認を事前に得て、個々の場合に応じて開示された情報。すべての機密情報は開示者の独占的資産であり、受領者は、本契約で明示的に規定されている場合を除き、これらの機密情報についていかなる権利やライセンスも保有しないものとします。

受領者は、本契約の条件に従って開示者の機密情報を適切に保護するために、機密情報の保護義務契約を書面で受領者と結んでいる担当者がやむを得ず機密情報を使用する必要がある場合を除き、機密情報の配布や開示を行わないこととします。また、受領者は、次の条件を満たしている場合に限り、法的な要件または裁判所の命令に応じて、開示者の機密情報を開示できる場合があることとします。(a) 開示要請を書面で開示者に迅速に通知すること。(b) 法的な要件または裁判所の命令で必要とされている範囲の機密情報だけを開示すること。(3) 開示する情報の複製を開示者に提供すること。

受領者は、自社の機密情報を保護する場合と同程度の注意を払って開示者の機密情報を保護する必要があります。受領者は、本契約で規定されている権利と義務に従い、必要な範囲でのみ開示者の機密情報を使用する必要があります。他の目的で開示者の機密情報を使用することはできません(使用する権利もありません)。また、受領者は、開示者の機密情報に対する偶発的または不正なアクセス、使用、変更、開示、改ざん、損失を防ぐための合理的かつ適切な技術的、物理的、組織的手段を実施する必要があります。また、保護する機密情報の所有、処理、特質に伴うリスクに対して、少なくとも合理的なレベルのセキュリティを確保する必要があります。こうした措置を行う場合は、該当する管轄権を有する行政機関の法律、規則、規制、命令(データ保護法で規定されている条項など。ただし、これらだけに限定されるものではありません)に準拠する必要があります。

本契約に従って転送、保存、または処理された機密情報に対する偶発的または不正なアクセス、破損、損失、改ざん、開示が発生したと考えられる場合、サプライヤーは、必ず 24 時間以内に NLL に通知することとします。この通知には、NLL が対象の機密情報の保護義務に準拠するために必要な情報と、不正な情報開示による損害を防止する(または最小化する)ための方法を記載する必要があります。サプライヤーは、NLL からの要請に応じて、全面的なサポートをすみやかに提供することとします。このサポートには、十分な知識を持つ主要な担当者にインシデント(個人データに関するデータプライバシーやセキュリティの問題など)の解決またはインシデントによる損害の軽減を担当させる、インシデントの影響範囲を特定する、インシデントとその根本原因を調査する、概要をまとめた書類を作成する、是正措置の実施を支援する(関係当局、影響を受ける関係者、公衆への告知等)などが含まれますが、これらだけに限定されるものではありません。

開示者からの特別な指示がない限り、受領者は開示者からの要請に応じて(または、サービスと本契約のいずれかが終了したときに)、すべての機密情報と、機密情報が含まれているデータや資料をすみやかに開示者に返却(または開示者から明示された指示によっては、破棄)することとします。NLL から要請があった場合、サプライヤーは 10 日以内に、本条項に記載されている条件に準拠していることを証明する書類を NLL に提出するものとします。この書類には、サプライヤーの役員または幹部による署名が必要です。

受領者は、機密情報と個人データの保護義務違反が、金銭的な損害を超える取り返しのつかない損害を開示者にもたらす可能性があり、本契約上の救済手段と権利に影響を与えることなく、開示者が公正な救済措置を求める権利を有していることに同意するものとします。

## 12. 情報セキュリティとデータ保護

情報セキュリティ: サプライヤーは、本契約の別紙 A (NLL のサプライヤーセキュリティ要件) で規定されている技術的かつ組織的な保護手段と管理手段以上の手段を講じていくことを表明するものとします。また、その時点における最新の業界標準に常に準拠するために、必要に応じてこれらの保護手段と管理手段をより高度なものへと改善していくこととします。

個人データとトラッキング: 第 17 項の「機密情報」に記載されているサプライヤーの義務に従い、サプライヤーが本契約に基づいて NLL のために(または NLL に代わって)個人データを処理する場合は、本契約の別紙 B として添付されている「データの取扱いに関する補足事項」の条件が適用されます。この場合の「処理」とは、手動的な方法であるか自動的な方法であるかを問わず、個人データまたは個人データのセットに対して実行する特定の操作や一連の操作のことを指しています。これらの操作には、個人データの収集、記録、編成、構造化、保管、適合、変更、取得、参照、使用、開示、転送、配布、有効化、調整、統合、制限、消去、削除などがあります。サプライヤーがサービスを実行する際に、トラッキング技術(ピクセル、タグ、Web ビーコンなど。ただし、これらだけに限定されるものではありません)を使用または提供する場合は、次の条件を満たしている必要があります。(i) 使用するトラッキング技術の種類と収集する情報について NLL に通知すること。(ii) サービスを実行するだけの目的で情報を収集して使用すること。(iii) トラッキング技術のオプトインとオプトアウトを行うための適切なメカニズムを使用すること。このメカニズムには、該当する法律に従い、情報を収集する前に正確で完全な開示を行うメカニズムなどが含まれますが、これらだけに限定されるものではありません。

## 13. 広報: サプライヤーは、NLL の広報部門から個々の場合に応じて書面による同意を事前に得ることなく、NLL の名前、ロゴ、

商標を使用したり、直接的であるか間接的であるかにかかわらず、NLL との関係、NLL が得るメリット、製品から得られるメリット、NLL との関係から得られるメリットについて言及したりすることはできません (また、本契約に従ってサプライヤーまたはサプライヤーの代理者が作成するドキュメント内でこれらについて言及することもできません)。

- 14. 行政機関との契約:** 本契約が米国政府 (または米国政府の下請契約) との主契約の履行に直接的または間接的に関連している場合、該当する規制 (連邦調達規則など) の条件が、本契約の対象となる契約または下請契約に挿入されます。
- 15. 輸出:** サプライヤーは、サービスの結果と製品を管理するための、該当するすべての国際法、国内法、連邦法、州法、地方自治体法などの規制や規則 (本契約を履行するための輸出免許に関する規制など) を順守するものとします。サプライヤーは、本契約に従い、すべてのソフトウェア、パーソナルコンピュータシステム、パーツ、技術データ、各種構成要素 (技術データと各種構成要素を「技術データ」と総称) について、直接的であるか間接的であるかを問わず、米国と他国の輸出管理法 (米国国務省が規定する指令 **Commence Denial and Probation Orders** や、米国財務省外国資産管理局が制定する制裁規定など) に違反する形で輸出や再輸出を行うことはできません。また、これらの指令や制裁規定に記載されている国、企業、個人に技術データを提供することもできません。事前に免許を取得することなく、該当する輸出入法で禁止されている国 (キューバ、北朝鮮、イラン、シリア、スーダンなど、貿易制裁の対象国。ただし、これらだけに限定されるものではありません) に対して、ソフトウェアと技術データの輸出や再輸出を行うことはできません。サプライヤーは、該当する輸出法に準拠するための内部的な手続きを維持する責任を負い、法的な要件に従って、サプライヤー自身が費用を負担する形でこうした法律を順守することに同意するものとします。サプライヤーは、本契約で規定されている義務を履行するために必要なすべてのライセンス、許可、承認を取得して維持し、該当する法律や規制に NLL が準拠するために必要なすべての情報 (米国輸出規制品目分類番号など、合理的な理由によって NLL が必要とする情報。ただし、これらだけに限定されるものではありません) を NLL に提供することとします。いずれかの当事者が本条項で規定されている条件に違反した場合は、本契約に対する重大な違反とみなされ、本契約を終了する正当な根拠になります。
- 16. 汚職防止法の順守:** サプライヤー、サプライヤーの役員、幹部、社員、請負業者、下請業者、代理店、サプライヤーに代わって行為を行う個人や事業体、サプライヤーの管理下で行為を行う個人や事業体は、該当する米国内の汚職防止法と国際的な汚職防止法 (連邦海外腐敗行為防止法や英国贈収賄防止法など。ただし、これらだけに限定されるものではありません) を順守するものとします。ビジネスの獲得や維持を行う目的、特定の個人または事業体にビジネスを振り分ける目的で、公的な収賄、商業的な収賄、脅迫の容認や黙認、リベットの受け取りなどの不正な手段を使用して支払を行ったり、価値の移転を行ったりすることはできません。サプライヤーは、この項で規定されている条件を順守する NLL の取り組みに全面的に協力し、NLL からの要請に応じて次のことを行うものとします (ただし、これらだけに限定されるものではありません)。(i) この項で規定されている条件に準拠していることを証明する書類を提出する (サプライヤーの代表者の署名が必要)。(ii) この項で規定されている条件に間する調査で、合理的で迅速なサポートをサプライヤーの費用負担で提供する。
- 17. その他**
- A. 準拠法、裁判地:** 国際物品売買契約に関する国連条約は、本契約には適用されないこととします。
- **南北アメリカ地域に拠点を置く NLL が締結した発注契約**は、法の抵触の原則に関係なく、カリフォルニア州の法律によって排他的に管理され、解釈されることとなります。この発注契約に基づいて発生する法的な措置や手続きは、カリフォルニア州サンタクララ郡でのみ実施されます。両当事者は、この人的管轄権と裁判地について同意するものとします。国際物品売買契約に関する国連条約は、本契約には適用されないこととします。
  - **欧州、中東、アフリカ地域に拠点を置く NLL が締結した発注契約**は、法の抵触の原則に関係なく、イングランドとウェールズの法律によって排他的に管理され、解釈されることとなります。この発注契約に基づいて発生する法的な措置や手続きは、英国の裁判所の管轄地でのみ実施されます。両当事者は、この人的管轄権と裁判地について同意するものとします。
  - **インドを含むアジア太平洋地域 (日本と中国を除く) に拠点を置く NLL が締結した発注契約**は、法の抵触の原則に関係なく、シンガポールの法律によって排他的に管理され、解釈されることとなります。この発注契約に基づいて発生する法的な措置や手続きは、シンガポールの裁判所でのみ実施されます。両当事者は、この人的管轄権と裁判地について同意するものとします。
- B. 可分性:** 本契約内のいずれかの条項の一部またはすべてが法律に違法または法的強制力がないと判断される場合、その条項は許容される最大限の範囲内で履行され、本契約で規定されているその他の条項の合法性と法的強制力については、完全な効力を持っているものとみなされます。
- C. 権利不放棄:** いずれかの当事者が本契約のいずれかの条項を履行できなかった場合であっても、該当する条項やその他の条項について、今後の履行を放棄したことはありません。本契約で規定されているすべての救済措置は排他的なものではないため、普通法または衡平法に基づく NLL の権利に影響を与えることはありません。

- D. 機会均等雇用者: サプライヤーは、次の要件に準拠することとします。(i) 機会均等雇用者として、人種、性別、年齢、出身国、障害、配偶者の有無、軍役経験の有無など、法律で禁じられている根拠によって個人を差別しないこと。(ii) こうした無差別ポリシーと、該当するすべての機会均等法やポリシーに準拠してすべての製品を提供すること。(iii) 直接的であるか間接的であるかにかかわらず、これらの法律とポリシーの規定や概念に違反しないこと。
- E. 条項の存続: 本契約で明示的に規定されている場合を除き、本契約上の権利と義務は、両当事者による本契約の履行の完了後も存続します(また、本契約の取消後や終了後も存続します)。これらの権利と義務には、支払い、所有権、機密情報、データ保護、当事者の関係、補償、責任の制限、広報、輸出、法律の順守に関する権利と義務が含まれますが、これらだけに限定されるものではありません。
- F. 実施:
- (i). 行動規範: サプライヤーは、常に **NLL** のグローバルサプライヤー行動規範を順守することとします。この行動規範の複製は、次の場所で参照することができます: <https://www.nortonlifelock.com/theme/procurement-code-conduct>
- (ii). **U.N.国連グローバルコンパクト**: **NLL** は、国連グローバルコンパクト(「グローバルコンパクト」)に加盟しています。**NLL** は加盟企業として、サプライヤーがグローバルコンパクトの 10 原則に従ってビジネスを行うことを奨励しています。これらの原則は、**NLL** 公式サイトの [Investor Relations] ページの [Corporate Governance] セクションで参照することができます。グローバルコンパクトは、人権、各国の労働法、労働環境、腐敗防止の分野で 10 個の普遍的な原則を推進するための国際的な取り組みです。詳しい情報については、[www.unglobalcompact.org](http://www.unglobalcompact.org) で参照することができます。
- G. 召喚状への対応: **NLL** の機密情報に関して、サプライヤーが特定の当事者から召喚状を受け取った場合、行政機関から情報提出の要請を受けた場合、または法的な要件により、**NLL** の機密情報を提出しなければならない場合(「召喚状」と総称)、サプライヤーは次の条件に従うこととします。(a) 召喚状を受け取ったことをただちに **NLL** に通知すること。(b) 召喚状を発行した当事者や行政機関に対して、同じ召喚状を **NNL** に直接送付するように依頼すること。(c) 召喚状を発行した当事者や行政機関が上記の依頼を拒否した場合は、機密情報の提出要請への対応において合理的な方法で **NLL** と協力し、召喚状に対するサプライヤーの対応をすべて記録してその複製を **NLL** に提供すること(こうした行為が許可されている場合)。

**NLL** が **NLL** の機密情報に関する召喚状を受け取った場合、サプライヤーは合理的な方法で **NLL** と協力し、**NLL** の機密情報を適時に提出するものとします。このような協力には、追加料金を受け取ることなく **NLL** の機密情報を収集して **NLL** に提供する、などの内容が含まれますが、これらだけに限定されるものではありません。こうした協力に関するサプライヤーの負担が合理的な範囲を超える場合、**NLL** とサプライヤーは、コストの適切な配分について誠実に交渉を行うこととします。

以上

これ以降のページに別紙 A (マスタープロバイダのセキュリティ要件) と別紙 B (データの取扱いに関する補足事項と添付資料) を掲載

**別紙 A**  
**NortonLifeLock Inc. およびその関連企業 (「NLL」と総称)**  
**マスタープロバイダのセキュリティ要件**

**1. NLLのセキュリティ要件**

サービスプロバイダ (「プロバイダ」) は、次の要件に準拠することとします。(i) この「マスタープロバイダのセキュリティ要件」文書に規定されている要件。(ii) 業界のベストプラクティスと標準の要件。(iii) 該当する法律と規制の要件。

本文書で規定されているいかなる要件も、NLLとプロバイダ間の合意、作業指示書、その他の条件(「合意」と総称)に基づくプロバイダのNLLに対する義務を制限するものではありません。これらの合意と本文書で規定されている要件が矛盾している場合、両当事者が署名した書面で明示的に合意した場合を除き、より厳しくレベルの高い保護基準が適用されるものとします。

**2. 定義**

用語	定義
NLL データ	NLL との合意に従い、プロバイダに提供される、またはプロバイダがアクセスできる NLL のデータ、コンテンツ、および情報。
制限付き NLL データ	<p>アクセスがごく少数だけに制限され、内容を知る必要がある場合にのみ共有される非常に機密性の高い NLL データ。</p> <p>法的要件や規制上の要件に従って保護する必要がある NLL データがこれに該当します。NLL が競争上の優位性を得る可能性のあるデータです。</p> <p>非公開の個人情報 (NPI)、個人を特定できる情報 (PII)、または保護対象保険情報 (PHI) が含まれている NLL データは、制限付き NLL データとみなされます。</p> <p>これらの情報を許可なく開示した場合、非常に大きな影響があります。制限付き NLL データへの不正なアクセス、使用、開示を行った場合、NLL に対する評価、法的な責任、財務面において大きな影響が発生することが予想されます。</p> <p>事業機会の損失や事業体制の変更などの大きな影響が発生し、事業の運営、資産、各社員にも大きな悪影響がおよぶことが予想されます。</p>
NLL 機密データ	<p>アクセスがプロジェクトチームなどの小規模グループだけに制限され、内容を知る必要がある場合にのみ共有される機密性の高い NLL データ。</p> <p>社外秘データや独自のコードなど、NLL が競争上の優位性を得る可能性のあるデータがこれに該当します。</p> <p>本条項で、制限付き NLL データ、NLL 機密データ、NLL 社外秘データ、ノートン LifeLock 社外秘データのいずれとしても分類されていないデータは、すべて NLL 機密データになります。</p> <p>NLL 機密データを許可なく開示した場合、非常に大きな影響があります。NLL 機密データへの不正なアクセス、使用、開示を行った場合、NLL に対する評価と財務面において大きな影響が発生する可能性があります。法的な影響が発生することは予想されません。</p> <p>事業機会の損失や事業体制の変更などの大きな影響が発生し、事業の運営、資産、各社員にも大きな悪影響がおよぶことが予想されます。</p>
NLL 社外秘データ	<p>事業を行うために使用される機密性の低い NLL データ。</p> <p>NLL 内での日常業務で一般的に使用されるデータがこれに該当します。</p> <p>このデータを許可なく開示した場合の影響は非常に限定的です。NLL 社外秘データへの不正なアクセス、使用、開示を行った場合、NLL に対する評価、法的な責任、財務面に対して影響が発生することは予想されません。</p> <p>事業機会の損失や事業体制の変更などによる影響は最小限で、事業の運営、資産、各社員に対する悪影響も非常に限定的です。</p>

用語	定義
処理	NLL データに対して実行される操作。自動的な方法かどうかに関係なく、収集、記録、使用、アクセス、コピー、複製、保持、保管、開示、変更、改変、転送、送信、削除、破棄などの操作のことを指します。これら以外にも、データの処分、販売、譲渡、ライセンス供与、マーケティングでの使用などについても、「処理」として分類されます。
担当者	プロバイダの社員、請負業者、下請業者。また、プロバイダと契約し、プロバイダに代わって NLL に対してサービスを提供したり、NLL の情報を取扱う第三者も「担当者」として分類されます。
NLL 情報資産	エンドユーザーのコンピューティングデバイス、ネットワーク、インフラストラクチャ、データリポジトリなどの NLL 資産。

### 3. 情報セキュリティポリシー

#### 3.1. 情報セキュリティの管理方針

3.1.1. プロバイダは 1 年に 1 回以上、経営幹部レベルで情報セキュリティポリシー (ISP) のレビューと承認を行うこととします。また、すべての担当者について ISP に準拠させることとします。

### 4. 情報セキュリティの組織

#### 4.1. 内部組織

4.1.1. プロバイダは、業界のベストプラクティスと標準に従って、物理的、技術的、組織的なセキュリティ対策を採用し、NLL に提供するプロバイダのサービスに適用されるすべての法的要件と規制上の要件に準拠するものとします。

### 5. 人事セキュリティ

#### 5.1. 採用前

5.1.1. プロバイダは、合意に基づく義務を制限することなく、法的に許容される範囲内で、制限付き NLL データ、NLL 機密データ、NLL ネットワークにアクセスできるすべての担当者について、NLL ポリシーに準拠して背景調査を実施することとします。この背景調査は、該当する規制や法律に従って実施する必要があります。次に示す調査に相当する調査を該当地域で実施する必要があります。社会保障番号追跡調査、グローバルブラックリスト調査、郡犯罪歴調査委 (5 年間の住所履歴)、連邦犯罪歴調査 (5 年間の住所履歴)、金融制裁調査。

#### 5.2. 雇用期間中

5.2.1. プロバイダは、業界のベストプラクティスと標準に従い、すべての担当者を対象として、セキュリティ意識向上トレーニングを 1 年に 1 回以上実施することとします。

#### 5.2.2. 追加のトレーニング

5.2.3. NLL から随時要請があった場合、プロバイダは追加のトレーニングを実施することとします。

#### 5.3. 退職と人事異動

5.3.1. 社員の退職や異動が発生した場合、または担当者がプロバイダの職務としてノートン LifeLock データを処理する必要がなくなった場合、プロバイダはそれらの社員や担当者について、ただちにアクセス権の削除や無効化などを行い、ノートン LifeLock データの制御権を適切に管理することとします。

### 6. 資産管理

#### 6.1. 資産に対する責任

6.1.1. NLL 情報資産を使用するプロバイダは、NLL の利用規定に厳密に従うものとします。

6.1.2. いかなる方法であっても、NLL との書面による合意を事前に得ることなく、NLL 情報資産を変更したり、他の当事者にサービスを提供する目的で NLL 情報資産を使用したりすることはできません。

#### 6.2. メディアの取り扱い

##### 6.2.1. 廃棄要件とコンプライアンスの証明書類

6.2.1.1. すべての NLL データは NLL の独占的資産であり、プロバイダは、該当する合意で明示的に規定されている場合を除き、これらのデータについていかなる権利やライセンスも保有しないものとします。プロバイダは NLL からの要請に応じて (または、該当する合意とサービスのいずれかが終了したときに)、すべての NLL データと、NLL データが含まれている情報や資料をすみやかに NLL に返却することとします (または、NLL が廃棄を指示することもあります。その場合も NLL の指示に従うこととします)。

6.2.1.2. プロバイダは、安全な方法でシステムとメディアを処分し、システムとメディアに含まれているすべての NLL データを解読不能または復元不能な状態にしてから、最終的な廃棄を行うこととします。これにより、NLL データがプロバイダの所有物では

なくなります。この廃棄は、NIST 承認基準に従い、NLL の要請を受けてから 10 日以内に行う必要があります。その際プロバイダは、廃棄の証明書類を NLL に提供することとします。

## 6.2.2. リムーバブルメディア

6.2.2.1. リムーバブルメディアの使用は禁止されています。NLL データを処理するすべてのワークステーションで、USB と外部ドライブ用のポートをすべて無効にする必要があります。

## 7. アクセス制御

### 7.1. アクセス制御のビジネス要件

7.1.1. プロバイダは、強力なアクセス制御の仕組みを導入し、制限付き NLL データまたは NLL 機密データを処理するシステムのオペレーティングシステム構成へのアクセスを、適切な権限を持つ許可された担当者だけに制限する必要があります。

### 7.1.2. モバイルデバイスと在宅勤務

7.1.2.1. プロバイダは、NLL データにアクセスできるすべての担当者について、プロバイダが貸与するデバイス (携帯電話を除く) を使用させることとします。

7.1.2.2. プロバイダは、担当者が携帯電話を使用して NLL データにアクセスすることを禁止する必要があります。

### 7.1.3. ユーザーアクセス管理

7.1.3.1. プロバイダは、システム (ネットワーク、ホスティング、アプリケーション) が最小権限の原則に従って設計されていることを確認するものとします。

7.1.3.2. プロバイダは、以下のように、すべてのシステム (ネットワーク、ホスティング、アプリケーション) で強力なパスワードを使用することとします。

- 長さが 10 文字以上のパスワード
- 次の文字のうち、3 つ以上の文字が含まれているパスワード: 大文字、小文字、数字、アルファベット以外の文字
- すべてのシステムで有効期間が 90 日に設定されたパスワード
- ハードコーディングされたり、ファイルに保存されたり、平文で保存されたり、平文で送信されたりすることがないパスワード

7.1.3.3. ソフトウェア製品とハードウェア製品内で使用されているベンダーのデフォルトパスワードは、インストール前またはインストール時にすべて変更する必要があります。

### 7.1.4. ユーザーの責任

7.1.4.1. 管理者アカウントの場合、プロバイダは、多要素認証の実行、パスワードの長さの増加、パスワードの有効期間の短縮、ユーザーの制限付きホワイトリストの使用など、制限の厳しい制御手段を使用して、管理者アカウントへのアクセスを制限することとします。

### 7.1.5. システムとアプリケーションのアクセス制御

7.1.5.1. プロバイダは、制限付き NLL データまたは NLL 機密データを処理するアプリケーションについて、関連するアプリケーション、アーキテクチャ、プロセスフロー、データフロー図、セキュリティ機能に関するドキュメントの維持管理を行うこととします。

## 8. 暗号技術

### 8.1. 暗号制御

8.1.1. プロバイダは、制限付き NLL データと NLL 機密データの送信や保存を行う場合に、NIST または PCI によって承認された暗号化標準とハッシュ標準 (SSH、SSL、TLS など) を使用することとします。

8.1.1.1. NLL データをノートパソコンに保管する必要がある場合、そのノートパソコンを完全なディスク暗号化で保護する必要があります。

8.1.2. 少なくともアーカイブシステムまたはバックアップシステムに保存された制限付き NLL データと NLL 機密データについては、実際の環境で使用されているデータと同じ保護手段で保護する必要があります。

## 9. 物理的なセキュリティと環境的なセキュリティ

### 9.1. 施設の安全確保

9.1.1. プロバイダは、制限付き NLL データまたは NLL 機密データが使用されるすべての施設 (データセンターやサーバールームなど。ただし、これらだけに限定されるものではありません) について、物理的なセキュリティと環境的なセキュリティを確保するものとします。プロバイダは、以下の要件に従う必要があります。

9.1.1.1. すべての担当者を対象として、役割、職務、スキルレベル、地理的な場所にに基づき、不正な物理的アクセスと論理的アクセスから情報資産を保護すること。

- 9.1.1.2. 対象となる施設とその他すべての該当エリアや設備 (バッジアクセスによって入退室が制御されている部屋、常時鍵がかかっている部屋、セキュリティ対策が導入されている施設、防犯カメラ、モニターアラームなど。ただし、これらだけに限定されるものではありません) について、担当者による入退室などの動作を管理、監視、記録すること。
  - 9.1.1.3. 熱、火災、水害などの環境ハザードから NLL データを保護すること。
  - 9.1.1.4. 施設への出入を監視するためのセキュリティ担当者を配置し、NLL データが施設内から持ち出されないようにするための厳格なポリシーを適用すること。
- 9.1.2. データセンター、コンタクトセンター、サーバーでは、NLL データを他の顧客データやテナントデータから論理的または物理的に分離する必要があります。

## 10. 運用セキュリティ

### 10.1. 運用手順と責任

- 10.1.1. プロバイダは、制限付き NLL データまたは NLL 機密データを処理するホストとインフラストラクチャについて、オペレーティングシステムの強化策を導入することとします。オペレーティングシステムの強化策としては以下の方法が考えられますが、これらだけに限定されるものではありません。
- 強力なパスワード認証
  - アイドルタイムアウト
  - 使用されていないポート/サービスの無効化
  - ログ管理
  - 不要なアカウントと期限切れアカウントの無効化または削除
  - アカウントのデフォルトパスワードの変更と、アカウントのデフォルト名の変更 (可能な場合)
  - ファームウェア、OS、システム、アプリケーション、データベースレベルのソフトウェアに対するタイムリーなパッチ適用とアップデート

### 10.2. マルウェアからの保護

- 10.2.1. プロバイダは、1 日 1 回以上署名をダウンロードするように設定された包括的なマルウェア対策ソリューションと、NLL ネットワークに接続するエンドユーザーコンピューティングデバイス、または制限付き NLL データや NLL 機密データを処理するエンドユーザーコンピューティングデバイス用のファイアウォールソリューション (またはその他の脅威保護技術) を導入し、維持管理を行うこととします。
- 10.2.2. プロバイダは、制限付き NLL データまたは NLL 機密データを処理するマシンでこれらの NLL データの使用、保存、持ち運びを行う場合に、外部デバイスの使用を禁止することとします。こうした外部デバイスには、フラッシュドライブ、CD、DVD、外付けハードドライブ、その他のモバイルデバイスなどがありますが、これらだけに限定されるものではありません。

### 10.3. ロギングとモニタリング

- 10.3.1. プロバイダは、システム監査またはイベントロギングと、それに関連する監視手順を実施して維持管理を行い、定期的なレビューを行う目的で、ユーザーアクセスとシステムアクティビティを記録することとします。すべてのログファイルを 12 カ月間以上保存し、適切な権限を持つ担当者以外にはログファイルへのアクセスを禁止する必要があります。
- 10.3.2. 制限付き NLL データまたは NLL 機密データに物理的にアクセスできるプロバイダは、CCTV、バッジリーダー、サインインシートのすべてのエントリポイントのログを維持管理することとします。すべてのログファイルを 12 カ月間以上保存し、適切な権限を持つ担当者以外にはログファイルへのアクセスを禁止する必要があります。

### 10.4. 脆弱性スキャン

- 10.4.1. 制限付き NLL データまたは NLL 機密データを取扱うプロバイダと、直接的であるか第三者経由であるかを問わず、インターネットからアクセス可能なサイトを NLL に代わってホストするプロバイダは、以下の要件に従う必要があります。
- 10.4.1.1. 業界標準のスキャンツールを使用して、ネットワーク、ホスト、アプリケーションの脆弱性を特定すること。
- 10.4.1.2. ネットワーク、ホスト、アプリケーションについて、内部脆弱性スキャンを毎月 1 回以上実行すること。
- 10.4.1.3. ネットワーク、ホスト、アプリケーションを実稼働環境にリリースする前と、ネットワーク、ホスト、アプリケーションの大幅な変更を行った後に、脆弱性スキャンを実行して脆弱性を特定すること。
- 10.4.1.4. CVSS スコアリングに従い、重大レベル、高レベル、中レベルの脆弱性をすべて修正してから、ネットワーク、ホスト、アプリケーションを実稼働環境にリリースすること。また、以下に示す期間に従い、次回の脆弱性のテストと修正を行うこと。
- 重大/高レベルの脆弱性 - 30 日以内
  - 中レベルの脆弱性 - 60 日以内
  - 低レベルの脆弱性 - 90 日以内
- 10.4.1.5. 重大なゼロデイ脆弱性が見つかった場合は、本条項の重大レベルの脆弱性で規定されている期間 (30 日) 以内に、推奨されるリスク軽減措置を実施すること。プロバイダは、推奨されるリスク軽減措置 (リスクソフトウェアパッチの適用、ソフトウェアのアップグレード、アプリケーション設定の変更、その他の補正的なセキュリティ管理方法) が公開され、安全にインストールして使用できるということがテストで実証されてから 12 営業日以内に、そのリスク軽減措置をすみやかに実施することとします。

## 10.5. 侵入テスト

- 10.5.1. 制限付き NLL データまたは NLL 機密データを取扱うプロバイダと、NLL ネットワークにアクセスするプロバイダは、以下の要件に従う必要があります。
- 10.5.1.1. 独立した第三者により、ネットワーク、ホスト、アプリケーションの侵入テストを1年に1回以上行うこと。
- 10.5.1.2. ネットワーク、ホスト、アプリケーションを実稼働環境にリリースする前と、ネットワーク、ホスト、アプリケーションの大幅な変更を行ってから30日以内に、独立した第三者によって侵入テストを実施すること。
- 10.5.1.3. 侵入テストで見つかった重大レベル、高レベル、中レベルの脆弱性をすべて修正してから、ネットワーク、ホスト、アプリケーションを実稼働環境にリリースすること。また、以下に示す期間に従い、次回の脆弱性のテストと修正を行うこと。
- 重大/高レベルの脆弱性 - 30日以内
  - 中レベルの脆弱性 - 60日以内
  - 低レベルの脆弱性 - 90日以内
- 10.5.1.4. 第三者によるネットワーク、ホスト、アプリケーション侵入テストの概要をNLLに提出すること。
- 10.5.1.5. 制限付き NLL データまたは NLL 機密データを取扱う、または NLL に代わってプロバイダのインターネットアクセス可能サイトをホストし、その使用状況をNLLに通知する、NLL に指名された下請業者または第四者の侵入テストレポートを確認すること。
- 10.5.1.6. NLL は、制限付き NLL データまたは NLL 機密データを取扱うプロバイダのネットワーク領域、NLL ネットワークに接続するプロバイダのネットワーク領域、またはインターネットからアクセス可能なサイトをホストするプロバイダのネットワーク領域で、NLL が個別に第三者を指名してネットワーク侵入テストを実行させる権利を有していることに同意すること。

## 11. 通信セキュリティ

### 11.1. ネットワークレベルの要件

- 11.1.1. プロバイダはファイアウォールを使用して、制限付き NLL データまたは NLL 機密データを処理するネットワークを保護するか、インターネットからアクセス可能なサイトを NLL に代わってホストする必要があります。このファイアウォールでは、ステートフルインスペクション、ロギング、すべての IPSec 標準と証明書サポート、強力な暗号化機能とハッシュのサポート、ICMP ベースおよび SNMP ベースの監視機能とスプーフィング防止機能を効率的に実行できる必要があります。プロバイダは、制限付き NLL データまたは NLL 機密データを処理するセグメントに対して、ネットワークベースのセキュリティモニタリングツール (syslog、セキュリティ情報とイベント管理 (SIEM) ソフトウェア、ホストベースの侵入検知システム) を導入することとします。
- 11.1.2. プロバイダは、外部に公開された Web サイトの IP アドレスで動的 DNS サービスを使用することはできません。静的 IP アドレスを使用できない場合は、インターネット以外の方法で対話や通信を行う必要があります。

### 11.2. ホスティングレベルの要件

- 11.2.1. プロバイダは、いかなる方法であっても (IaaS、PaaS、SaaS、データの処理、送信、アクセス、保存など)、NLL からの書面による明確な同意を事前に得ることなく、クラウド環境を使用したり変更したりすることはできません。NLL がクラウド環境の使用や変更を許可した場合、プロバイダはすべての制限付き NLL データと NLL 機密データを論理的に分離することとします。

### 11.3. 情報の転送

- 11.3.1. プロバイダは、米国以外の場所で、NLL データへのアクセス、保存、処理、使用を行わないこととします。また、プロバイダは、NLL データにアクセスするすべての担当者が米国に居住していることを確認するものとします。NLL データへのアクセスや処理を米国以外の場所で行う場合は、追加の条件や合意が必要になることがあります。その場合プロバイダは、NLL が随時要請する可能性がある追加の条件や合意を迅速かつ誠実に締結することに同意するものとします。

## 12. システムの取得、開発、保守

### 12.1. 開発プロセスとサポートプロセスのセキュリティ

- 12.1.1. NLL 向けソースコード (NLL 製品や NLL サービスのソースコードなど。ただし、これらだけに限定されるものではありません) の開発や処理を行うプロバイダと、制限付き NLL データまたは NLL 機密データを処理するアプリケーションの開発と保守を行うプロバイダは、以下の要件に従う必要があります。
- 12.1.1.1. 該当するサービスを NLL に提供する目的で、対象となるすべての担当者に対して、セキュアなコードを記述するためのトレーニングを1年に1回以上実施する必要があります。開発者は、OWASP Top 10 と CWE/SANS Top 25 の脆弱性と、それらの脆弱性の適切な修正技術に精通している必要があります。プロバイダは、NLL との間で合意を締結してから30日以内に、これに準拠していることを示す証明書類をNLLに提出し、その後毎年同様の証明書類を提出することとします。
- 12.1.1.2. 文書化された変更管理プロセスとソフトウェア開発ライフサイクル (SDLC) の年次レビューを行い、それを証明する書類をNLLに提出する必要があります。この年次レビューでは、以下のレビューを行います。
- 個別のセキュアコードレビュー

- アプリケーションを開発するためのセキュアプログラミングのガイドラインとプロトコルのレビュー
- アプリケーションやソースコードに対する主要なリスクを特定するための脅威モデルメソッドロジーのレビュー
- アプリケーションセキュリティテストのレビュー (このテストには、静的アプリケーションセキュリティテスト (SAST)、動的アプリケーションセキュリティテスト (DAST)、第三者による侵入テストが含まれる場合があります)

## 12.2. テストデータ

12.2.1. プロバイダは、いかなるテストシナリオにおいても、NLL データを使用することはできません。

## 13. サプライヤーとの関係

### 13.1. サプライヤーとの関係における情報セキュリティ

- 13.1.1. NLL ネットワークに接続するプロバイダ、制限付き NLL データまたは NLL 機密データを取扱うプロバイダ、インターネットからアクセス可能なサイトの開発やホスティングを NLL に代わって行うプロバイダは、該当する SOC 2 Type 2 認証または ISO/IEC27001 認証 (あるいはこれら両方) の維持管理を行うこととします。また、SOC 2 Type 2 報告書または ISO27001 適用宣言書 (あるいはこれら両方) を証明書とともに NLL に提出することとします。
- 13.1.2. 上記の証明書類を提出できないプロバイダは、NLL が実施するセキュリティリスク評価 (SRA) を受けるか、SIG LITE を提供する必要があります (あるいはこれら両方)。いずれも、毎年 1 回実施することとします。
- 13.1.3. NLL は、PCI レベル 1 のマーチャントです。NLL に代わってクレジットカードデータを取扱うプロバイダは、本合意に基づいて提供されるサービスに対してペイメントカード業界データセキュリティ基準 (PCI DSS) が適用される範囲において、常に最新バージョンの PCI DSS に準拠することとします (たとえば、PCI DSS で定義されているカード所有者データや、PCI DSS の保護対象となるその他のデータ (「PCI データ」と総称) について、アクセス、収集、使用、保持、処理、開示、転送などを行う場合や、いずれかのサービスが PCI データ環境のセキュリティに影響する場合など)。プロバイダは、NLL からの要請に応じて、PCI-DSS に準拠していることを証明するための書類をすみやかに NLL に提出することとします (この証明書類は、NLL が独自の裁量で決定することとします)。PCI DSS に対する潜在的な違反が発生していることにプロバイダが気付いた場合、プロバイダは、そうした違反に気付いてから 48 時間以内に NLL に通知し、NLL が指定する期間内 (遅くとも、違反に気付いてから 30 日以内) にその違反を是正し、PCI DSS に準拠する必要があります。プロバイダは、自社のすべての担当者について、本合意でプロバイダへの適用が規定されているすべての義務を負うことと、本合意を順守する責任を NLL に対して負うことを保証するものとします。プロバイダは、NLL との間で合意を締結してから 30 日以内に、これに準拠していることを示す証明書類 (PCI AoC) を NLL に提供し、その後毎年同様の証明書類を提出することとします。
- 13.1.4. 合理的な理由により、プロバイダまたはプロバイダの担当者が、NLL データが侵害された可能性があると判断した場合 (許可されていない方法で NLL データが処理された場合など。ただし、これらだけに限定されるものではありません)、NLL は 3 日前に通知することにより、サプライヤーの費用負担で SRA を実施できるものとします。SRA を実施する場合、プロバイダはすみやかに、誠実で全面的なサポートを提供することとします。
- 13.1.5. プロバイダとプロバイダの担当者は、NLL または NLL が任命する第三者監査人 (NLL や NLL 関連企業の規制調査機関など) と全面的に協力し、NLL または第三者監査人が次の項目にアクセスすることを許可するものとします。(i) サービスの実行または NLL データの取扱いに関与する担当者。(ii) サービスが実行されている施設。(iii) サービスを実行するためのアプリケーションとシステム。(iv) サービスに関して作成または保存されたデータとレコード、またはプロバイダと NLL またはプロバイダとプロバイダ担当者 (あるいはこれら両方) との間で締結された合意に従って作成または保存されたデータとレコード。
- 13.1.6. 書面による同意を NLL から事前 to 得ることなく、制限付き NLL データやノートン LifeLock 機密データを他の第三者と共有することはできません。

### 13.2. 監査権

- 13.2.1. NLL は、関連する合意に記載されている NLL の調査権と監査権のほかに、プロバイダに対して NLL のセキュリティリスク評価を 1 年に 1 回以上実施するように要請する権利を有しています。プロバイダが妥当な期間内にこうした要請に応じなかった場合、またはセキュリティに関する調査の結果、NLL のセキュリティの問題への対処について、NLL が要求するレベルをプロバイダが満たしていないことがわかった場合、NLL は、他の監査権やその他の権利のほかに、信頼できる第三者監査人に SRA の実施を依頼する権利を有しています。

## 14. 情報セキュリティインシデント管理

### 14.1. 情報セキュリティインシデントの管理と改善

- 14.1.1. 合理的な根拠により、制限付き NLL データまたは NLL 機密データが不正に処理された可能性があるとして判断した場合 (許可されていない方法でデータが処理された場合など。ただし、これらだけに限定されるものではありません)、プロバイダは 24 時間以内に NLL に通知することとします。
- 14.1.2. プロバイダは、以下の情報を NLL に以下を通知することとします。
- 14.1.2.1. インシデントのカテゴリとおおよその規模など、インシデントの概略的な情報
- 14.1.2.2. 詳細な情報を知っているプロバイダ担当者の氏名と連絡先
- 14.1.2.3. インシデントに対して実施する措置またはその提案 (インシデントによる悪影響を軽減するための措置など)

14.1.3. プロバイダは必要に応じて、すみやかに NLL と協力して関連する調査を行い、インシデントの解決に誠実に取り組むこととします。

## 15. 事業継続性管理における情報セキュリティ

### 15.1. 情報セキュリティの継続

- 15.1.1. プロバイダは、NLL に対して実行されるサービスについて、事業継続計画 (BCP) と災害復旧計画 (DRP) (「計画」と総称) の維持管理を行うことに同意するものとします。
- 15.1.2. 計画のテストを 1 年に 1 回以上実施する必要があります。NLL は、テスト結果のコピーの提出を要請する場合があります。プロバイダは、NLL が指摘したすべての項目を修正することとします。
- 15.1.3. プロバイダの計画には、少なくとも以下の要件が含まれている必要があります。
- 15.1.3.1. 事業継続計画 (BCP)。プロバイダは、重要な事業について BCP を確保する必要があります。BCP には、重要な各事業の復旧を計画するために必要な情報が含まれている必要があります。復旧方法を実行するための要件を、BCP として文書化する必要があります。BCP には、関連するビジネス影響度分析で定義された、重要な事業の復旧タイムラインを達成するための方法を含める必要があります。BCP には、以下の情報を含める必要があります。
- 概要:
    - 計画の概要 (具体的な復旧目標など)
    - 範囲
    - 想定条件
    - ビジネス影響度分析 (BIA)
  - 以下に示す各影響に対する詳しい復旧方法と復旧手順:
    - 施設の損失
    - 重要な担当者の損失
    - 核となる依存関係の損失
  - 通知、エスカレーション、計画をアクティブ化する手順
  - 連絡先リスト
  - リソース復旧の要件
- 15.1.3.2. 災害復旧計画 (DRP)。DRP では、以下の要件が適用されます。ただし、以下の要件よりも厳格な要件が本合意に記載されている場合は、その要件が適用されます。
- プロバイダは、NLL からの要請に応じて、NLL の Web サイトとデータをホストするためのサイト、ネットワーク、システム、アプリケーションに関する DRP を 30 日以内に NLL に提出することとします。
  - 提出する DRP には、4 時間以内の目標復旧時間 (RTO) と 1 時間以内の目標復旧時点 (RPO) を達成するための手順が記載されている必要があります。
- 15.1.3.3. インターネットサービスプロバイダ: プロバイダは、2 社以上のインターネットサービスプロバイダ (ISP) と契約して、自社の建物への通信経路を複数確保することにより、トラフィックが自動的に別の ISP に転送されるようにする必要があります。
- 15.1.3.4. 火災: プロバイダの施設には、機器やシステムに影響を与えることなく、すみやかに消火できる自動消火システムが導入されている必要があります。
- 15.1.3.5. 帯域幅: プロバイダは、2 つの同じルーターと代替ファイアウォールサーバーを使用することとします。バックアップ用のルーターとファイアウォールは、即時にオンライン状態に移行できるように設定されている必要があります。
- 15.1.3.6. 電源: プロバイダのサービス施設では、ヘビーデューティユーティリティフィード、大規模な無停電電源装置 (UPS) バッテリーバックアップ、電源と UPS 間のサージ防護機器、バックアップジェネレーターなど、複数の電源を確保する必要があります。
- 15.1.3.7. サーバー障害: プロバイダのシステムでは、稼働時間と保守の要件を満たすために必要な合理的な冗長性を確保する必要があります。
- 15.1.4. プロバイダは、計画上で定義された災害が発生したと判断した場合、ただちに NLL に通知し、計画に従って担当する活動を開始することとします。プロバイダが、本条項で規定されている災害復旧サービスの実施義務に実質的に違反し、その結果として、NLL の事業運営に不可欠なサービスを所定の期間内に開始できなかった場合、NLL は、災害が継続している間は、本合意に基づく NLL の権利のほかに、第三者に当該サービスの実施を依頼する権利を有することとします。災害が停止したら、プロバイダは合理的な範囲で可能な限りすみやかに、災害の理由と、災害を解決するためにプロバイダが講じたすべての措置が詳しく記載されたインシデントレポートを NLL に提出することとします。

**別紙 B**  
**データの取扱いに関する補足事項**

NortonLifeLock Inc. またはその関連会社（「NLL」と総称）あるいはこれら両方は、プロバイダによる個人データの取扱いに関する合意に基づいて、プロバイダから特定の製品またはサービスを（あるいはこれら両方）を調達しました。

この場合、NLL は個人データに関して「管理者」という立場になり、プロバイダは「処理者」という立場になります。または、NLL が関連会社などのエンドカスタマーに対する「処理者」（最終的なデータ管理者）になり、プロバイダが、NLL の指示に従ってエンドカスタマーと直接やり取りをする「復処理者」になる場合もあります。

両当事者は、以下のとおり合意するものとします。

- 1. 定義:** 本合意で特に定義されていない限り、この項で太字で記載されているすべての用語は、その用語に続いて記載されている意味を持つこととします。本補足事項に記載されている用語の定義が、該当するデータ保護法で規定されている定義と矛盾する場合は、データ保護法の定義が優先されるものとします。

「**該当する EU の法律**」とは、次の法律のことを指しています。(i) 個人データの取扱いと個人データの自由な移動に関する 1995 年 10 月 24 日付欧州議会および理事会の 95/46/EC 指令、(ii) 個人データの処理に関する自然人の保護と個人データの自由な移動に関する 2016 年 4 月 27 日付欧州議会および理事会の EU 一般データ保護規則 2016/679 (2018 年 5 月 28 日時点) と、95/46/EC 指令に代わる新しい GDPR 規則、(iii) 該当する欧州連合加盟国法規。

「**管理者**」とは、個人データを処理する目的と処理方法を単独で（または他者ととともに）決定する当事者のことを指しています。

「**データ保護法**」とは、該当する EU の法律と、本合意に基づいて処理される個人データに適用される可能性があるその他のデータ保護法のことを指しています。

「**EEA**」とは、欧州経済領域のことです。

「**個人データ**」と「**データ主体**」は、本合意に記載されている同じ意味を持つ用語です。

「**個人データ侵害**」とは、転送、保管、または処理された個人データの偶発的または不正な破損、損失、改ざん、開示、アクセスにつながるセキュリティ違反のことを指しています。

この場合の「**処理**」とは、手動的な方法であるか自動的な方法であるかを問わず、個人データまたは個人データのセットに対して実行する特定の操作や一連の操作のことを指しています。これらの操作には、個人データの収集、記録、編成、構造化、保管、適合、変更、取得、参照、使用、開示、転送、配布、有効化、調整、統合、制限、消去、削除などがあります。

「**処理者**」は、本合意に記載されている意味を持つ用語です。

「**サービス**」とは、本合意に記載されているサービスのことを指しています。

「**標準契約条項**」とは、95/46/EC 指令に従って第三国の処理者に転送される個人データに関する標準的な契約条項について、2010 年 2 月 5 日に行われた欧州委員会の決定に基づいて規定された条項のことです。これらの条項のフォームを、付録 1 として本書に添付します。

- 2. 法令順守:** 各当事者は、該当するデータ保護法を順守することとします。具体的には、本合意に規定されている要件を制限することなく、NLL は、該当する EU の法律に従って管理者としての義務を果たし、プロバイダは、該当する EU の法律に従って処理者としての義務を果たすこととします。データ保護法で要求される範囲において、両当事者は誠意をもって交渉を行い、本合意に基づくサービスの提供に必要な個人データの取扱いに関する追加の文書、補足文書、改訂文書を作成することに同意するものとします。

- 3. データの処理:** プロバイダは、NLL または NLL 関連企業から書面での指示を受けない限り、個人データを取扱うことはできません。ただし、プロバイダに適用されるデータ保護法によって個人データを取扱う必要がある場合を除きます。その場合、プロバイダまたはプロバイダの関連企業は、個人データを取扱う前に、該当するデータ保護法によって許可される範囲で、そのデータ保護法の法的要件を NLL に通知することとします。NLL と NLL の各関連企業は、プロバイダとプロバイダの各関連企業に対して、次のことを指示します（また、復処理者にも同じ指示を出すように、プロバイダとプロバイダの関連企業に要請します）。(i) サービスの一部として個人データを取扱うこと。(ii) 特に、サービスの提供に必要な個人データを特定の国や地域に転送する場合は、必ず本合意で明示的に規定されている要件に準拠すること。NLL は、NLL 自身と NLL 関連企業に代わり、該当するすべてのケースで、本条項に記載されている指示を出すための権利を有していることを保証し、表明します。

両当事者は、該当する各作業指示書に、個人データの処理の性質、目的、期間、内容を記載することとします。内容としては、個人データのカテゴリ、データ主体のカテゴリ、サービスの一部として個人データを取扱う復処理者の一覧（復処理者が個人データを取扱う場合）、プロバイダが個人データを取扱う場所、各復処理者が個人データを取扱う場所（復処理者が個人データを取扱う場合）などを記載します。

- 4. プロバイダの社員/代理店:** プロバイダは、個人データへのアクセスを、本合意に従って個人データを取扱う必要のある社員と代理人だけに制限することとします。また、個人データにアクセスするこれらの社員と代理店について、次の要件に従うことに同意するものとします。(i) 個人データの機密を守ること。(ii) この別紙に記載されているデータ守秘義務と、該当するデータ保護法に準拠すること。個人データにアクセスする社員や代理店が担当業務から外れる場合、プロバイダは、それらの社員と代理店について、個人データへのアクセスまたは個人データを処理するシステムへのアクセス（あるいはこれら両方）を禁止する必要があります。

- 5. データ主体の権利と管理者による支援:** プロバイダは、NLL の個人データについて、データ主体または他の当事者から受け取った要求を NLL に通知することとします。プロバイダは、こうした要求に直接対応することはできません。ただし、NLL の書類で規定されている場合や、該当するデータ保護法で規定されている場合を除きます。このような場合、プロバイダは、該当するデータ保護法で許可される範囲で、個人データの要求に対応することとします。プロバイダは、準拠すべきデータ保護法の要件に従い、合理的な方法で NLL を支援する必要があります。こうした要件には、データ主体の要求に対応するための NLL の義務、データ主体の権利の透明性と履行に関する NLL の義務などがありますが、これらだけに限定されるものではありません。

6. **技術的かつ組織的なセキュリティ対策:** プロバイダは、最新の技術、導入のコスト、データ処理の性質、範囲、コンテキスト、目的、自然人の権利と自由に対するさまざまな可能性と重大性のリスクを考慮して、適切な技術的かつ組織的セキュリティ対策（該当するデータ保護法（GDPR）の第32条1項など）で規定されている対策などを導入し、対象となるリスクに適したレベルのセキュリティを確保することとします。プロバイダは、本合意の要件を制限することなく、本合意の別紙 B に記載されているセキュリティ対策を実施することに同意するものとします。
7. **技術的かつ組織的なセキュリティ対策の監査:** プロバイダは NLL からの要請に応じて、本合意に基づいて適用されるデータ保護ポリシーとデータ保護手順に準拠していることを証明するために必要なすべての情報を提出することに同意するものとします。これらの情報には、プロバイダが実施したその時点における最新の監査の結果、認定書、証明書（例: ISO 27001、SOC2 TYPE2）などがありますが、これらだけに限定されるものではありません。該当するデータ保護法、データ保護機関、または規制当局が規定する要件に従い、NLL、第三者のデータ管理者、または第三者のデータ処理者が、監査目的でプロバイダの担当者、データ、システム、施設に関する追加情報または物理的なアクセスが必要な場合、別紙 B に記載されている監査規定とアクセス規定に基づき、機密保持義務に合意した上でそうした物理的なアクセスを行うこととします。
8. **データ侵害に関する通知と修復:** 個人データの侵害があった場合、プロバイダは、すべてのケースにおいて 24 時間以内に NLL に通知することとします。その際、プロバイダは、個人データに対する既知の違反または違反が疑われるケースについて、次のメールアドレスにすべての通知を送信することとします。 [security@nortonlifelock.com](mailto:security@nortonlifelock.com)

個人データの侵害が発生した場合、プロバイダは、NLL が法律で規定されている義務（GDPR の第 33 条や第 34 条など。ただし、これらだけに限定されるものではありません）に準拠するために必要なすべてのサポートと協力を合理的な方法で NLL に提供することとします。また、プロバイダは、合理的な方法で可能な限りすみやかに、プロバイダがすべての費用を負担する形で必要なすべての合理的措置を講じて、個人データ侵害の根本原因を特定し、個人データに対するその後の不正アクセス、使用、処理を防止することとします。プロバイダは、NLL からの要請に応じて、全面的なサポートを迅速に提供するものとします。このサポートには、該当するログやシステムを使用し、十分な知識を持つ主要な担当者に個人データに関するプライバシーの問題やセキュリティの問題（またはこれらの問題による損害の軽減）を担当させる、インシデントの影響範囲を特定する、インシデントを調査する、概要をまとめた書類を作成する、追加の是正措置の実施を支援する（データ保護法や NLL が規定する要件に従い、関係当局、影響を受けるデータ主体、公衆に合理的に必要とされる告知をするなど。ただし、これらだけに限定されるものではありません）などが含まれますが、これらだけに限定されるものではありません。法律で明示的に要求されている場合、または第三者との合意で規定されている場合を除き、プロバイダは、NLL から書面による同意を事前に得ることなく、NLL の個人データがデータ侵害に関与したことを第三者に通知しないことに同意するものとします。法的な要件または第三者との合意により、個人データ侵害の事実を公衆または第三者に通知せざるを得ない場合、プロバイダは、直接的であるか間接的であるかを問わず、データ侵害の当事者として NLL を特定しないこととします。また、NLL、NLL の顧客、NLL の社員に対する悪影響を最小限に抑えるため、商業的に合理的な努力を払い、データ侵害に関する通知内容について、NLL から事前に承認を得ることとします。NLL は、プロバイダによる個人データへのアクセス、処理、保存について、中断や終了を指示する場合があります。また、既知の個人データ侵害やデータ侵害が疑われるケースに対して、適切な措置を講じる場合があります。

プロバイダは、プロバイダが本合意に違反したこと起因する個人データ侵害について、NLL に対する第三者からのあらゆる申し立て、訴訟、措置、訴訟手続き、要求、判断、損失、支払い、費用（調査費用、第三者による技術的な費用、合理的な弁護士費用など）、損害、和解、責任、罰金、罰則から、NLL、NLL の代理者、譲受人、後継者の保護と補償を行うこととします。プロバイダは、本合意で規定されている権利と、法律または衡平法によって認められている NLL のその他の権利と救済策を制限することなく、プロバイダが引き起こした個人データ侵害の結果として NLL が被った実際の費用と責任について、その全額を NLL に払い戻すこととします。これらの費用には、個人データ侵害の調査とデータ修復に関して NLL が負担した費用や、個人データが侵害された可能性のあるデータ主体に対する通知や信用調査の費用などが含まれますが、これらだけに限定されるものではありません。

9. **データの復処理:** プロバイダは、サービスを提供する目的で個人データを取扱う復処理者を第三者プロバイダとして契約する前に、NLL から書面による同意を得る必要があります。NLL は、本合意で規定されている要件を制限することなく、NLL 自身と NLL の関連企業に代わり、付録 1 に記載されている復処理者を使用することに同意します。本合意の有効期間内に新しい復処理者を任命する場合、プロバイダは、その復処理者が本合意に従って個人データにアクセスする日の 45 日前までに、NLL に通知することとします。NLL は、通知を受け取ってから 60 日以内であれば、新しい復処理者の任命に反対することができます。NLL がこの条件に従って新しい復処理者の任命に反対した場合、プロバイダは商業的に合理的な努力を払ってサービスを変更し、その復処理者が NLL の個人データを使用できないようにする必要があります。プロバイダがサービスを変更できない場合、NLL は、本合意の条件に従って書面による通知を提出することにより、該当するサービスを終了する場合があります。本条項の規定に従ってサービスが終了した場合、プロバイダは、未使用の前払い料金について、比例計算で払い戻しを行うこととします。

プロバイダは、復処理者が行うデータ取扱い操作を、サービスを提供するために必要不可欠な操作だけに制限する必要があります。プロバイダは、この別紙に記載されている要件と同等以上のデータ保護要件を書類として作成し、復処理者にそれらの要件を順守させることとします。また、この別紙で規定されているデータ保護義務に準拠する義務を負うこととします。

10. **EEA+ におけるデータ転送とデータの取扱い:** プロバイダは、付録 1 に記載されている場所でのみ個人データを取扱うこととします。NLL から書面による許可を事前に得ることなく、個人データを国外に転送することはできません。当事者間で合意したデータ転送の方法を変更する場合、プロバイダは、その変更について NLL に通知し、NLL の同意を得る必要があります。欧州経済領域（EEA）または欧州経済領域にスイスを加えた領域（EEA+）で発生した個人データのうち、本合意に従ってプロバイダが処理を行い、EEA+ 外に転送する可能性があるデータについて、両当事者はデータ処理の詳細を合意文書として作成し、EU 標準契約条項で規定されている条件（付録 2 として添付）に従い、NLL 関連企業とプロバイダ間でデータ転送を管理することとします。こうしたデータ転送の方法が適切ではないと考えられる場合、プロバイダは、EEA + の外部に転送されるデータを保護するための適切な方法であると NLL が判断したデータ転送方法を実行することに同意するものとします。第 9 条の条件に従い（該当する場合は、EU の法律にも従い）、データ保護に関する法規制が EEA+ よりも緩やかな国に拠点を置く復処理者に EEA+ の個人データを転送する場合、プロバイダは、該当する EU 法規で代替手段による個人データの転送が許可されている場合を除き、付録 2 に記載されている EU 標準契約条項に従い、NLL に代わって復処理者にデータを転送することとします。

11. **データ保護影響評価と事前協議:** プロバイダは、データ保護影響評価と、規制当局、監督当局、データ保護機関との事前協議について、合理的なサポートを NLL に提供することとします。NLL は合理的な理由により、これらの評価と協議を、該当するデータ保護法による要件として認識しています。いずれの場合も、プロバイダによる個人データの取扱いにのみ関係しています (取扱いと情報の性質が考慮されます)。
12. **コンプライアンス:** プロバイダは、自社の業務が本合意で規定されている条件に準拠しているかどうかを常に確認し、プロバイダの担当者、代理店、復処理者について、個人データを取扱うための資格を持ち、適切なトレーニングを受け、データの取扱いに対する責任を負うことを保証するものとします。また、個人データを取扱う前に、個人データにアクセスする個人について、該当する法律で許可される範囲で、適切な背景調査とレビューを行うこととします。プロバイダは、本合意で規定されている要件に従い、個人データの取扱いと保護を行うプロバイダの担当者、代理店、復処理者に対して、データ保護に関する法律と規制、個人データの保護義務について説明し、適切なトレーニングを実施する必要があります。プロバイダは、プロバイダの担当者、代理店、復処理者がデータ取扱いの担当から外れた場合、それらの担当者、代理店、復処理者による個人データへのアクセスと個人データを処理するシステムへのアクセスをただちに禁止することに同意するものとします。
13. **個人データの返却または削除:** NLL から書面による要求を受け取った場合、プロバイダは NLL の指定に従い、妥当な期間内に個人データを削除または返却することとします。NLL から要求があった場合、プロバイダは別紙 A に記載されているマスタープロバイダのセキュリティ要件に従い、個人データの返却と削除に関する規定に準拠していることを証明する書類を NLL に提出する必要があります。
14. **優先順位:** 本合意とこの別紙との間に矛盾がある場合、この別紙に記載されている条件が優先されます。

添付資料:

付録 1 - 標準契約条項 (付属書類 1 と 2 を添付)

## 付録 1

### 欧州委員会決定 C(2010)593 標準契約条項 (処理者)

EU データ保護指令 (Directive 95/46/EC) 第 26 条 2 項に関する、十分なレベルの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ついての標準契約条項

データ輸出組織: NortonLifeLock Inc. またはその関連企業。住所: .....

電話番号: .....FAX: .....メールアドレス:

(これ以降は「データ輸出者」と表記)

及び

データを受信する組織は、本合意 (または、本合意に従って実施される作業の指示書) に明記されているプロバイダまたはその関連企業である。住所:

電話番号: .....FAX: .....メールアドレス: .....

(これ以降は「データ輸入者」と表記)

各々を「各当事者」、両者を合わせて「両当事者」という。

上記の者は、データ輸出者からデータ輸入者に対する個人データ (付属書類 1 に明記されているもの) の移転における、個人のプライバシー、基本的権利及び自由の保護に関する十分な保護措置を提示するため、以下の契約条項 (以下「本契約条項」という) に合意した。

## 第 1 条

### 定義

本契約条項において、以下の用語は、以下の意味を有するものとする。

- (a) 「個人データ」、「特別カテゴリーのデータ」、「処理」、「管理者」、「処理者」、「データ主体」及び「監督当局」は、個人データ取扱いに係る個人の保護及び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指令 (Directive 95/46/EC) における定義と同じ意味を有する。
- (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する。
- (c) 「データ輸入者」とは、データ輸出者の指示及び本条項の条件に従い、移転した後にデータ輸出者に代わって処理を行うことが予定されている個人データを、データ輸出者から受領することに同意する処理者であり、Directive 95/46/EC の第 25 条 (1) 項での意味における十分な保護を提供する第三国の制度に服していない者を意味する。
- (d) 「復処理者」とは、データ輸入者又はデータ輸入者の他の復処理者から業務を請け負う処理者であり、移転した後に、データ輸出者の指示、本条項の条件及び書面による契約の条件に従い、データ輸出者に代わって処理を行うことのみを目的とした個人データを、データ輸入者又はデータ輸入者の他の復処理者から受領することに同意した者を意味する。
- (e) 「該当するデータ保護法」とは、データ輸出者が設立された EU 加盟国においてデータ管理者に適用される、個人の基本的権利及び自由 (特に、個人データの取扱いに関するプライバシー権) を保護する法律を意味する。
- (f) 「技術的かつ組織的セキュリティ対策」とは、特にネットワークを通じた送信による処理が行われる場合の偶発的又は違法な破壊、偶発的な喪失、変更、不正開示又はアクセス、及びその他のあらゆる違法な処理形態から個人データを保護することを目的とする対策を意味する。

## 第 2 条

### データ移転の詳細

データ移転 (該当する場合は、とりわけ特別カテゴリーの個人データ) の詳細は、付属書類 1 (同付属書類は、本契約条項の不可分な一部を構成する) において特定される。

### 第3条

#### 第三者受益条項

1. データ主体は、第三受益者として、データ輸出者に対し、本条、第4条(b)項～(i)項、第5条(a)項～(e)項及び(g)項～(j)項、第6条(1)項及び(2)項、第7条、第8条(2)項、第9条～第12条を行使することができる。
2. データ主体は、データ輸出者が事実上消滅し、又は法律上存在しなくなった場合、データ輸入者に対し、本条、第5条(a)項～(e)項及び(g)項、第6条、第7条、第8条(2)項、第9条～第12条を行使することができる。ただし、データ輸出者の承継人が、契約又は法律により、データ輸出者の法的義務を全て引き受け、その結果、当該承継人がデータ輸出者の権利義務を承継した場合を除く。この場合、データ主体は、当該承継人に対してこれらを行使することができる。
3. データ主体は、データ輸出者及びデータ輸入者の双方が事実上消滅し、もしくは法律上存在しなくなった場合、又はこれらの双方が支払不能に陥った場合、復処理者に対し、本条、第5条(a)項～(e)項及び(g)項、第6条、第7条、第8条(2)項、第9条～第12条を行使することができる。ただし、データ輸出者の承継人が、契約又は法律により、データ輸出者の法的義務を全て引き受け、その結果、当該承継人がデータ輸出者の権利義務を承継した場合を除く。この場合、データ主体は、当該承継人に対してこれらを行使することができる。データ復処理者の第三者に対する法的責任は、本契約条項に基づく自身の処理業務に限定されるものとする。
4. 両当事者は、データ主体が希望し、かつ国内法上許容されている場合は協会又はその他の機関がデータ主体を代理することに異議を申し立てない。

### 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、以下を保証する。

- (a) データ輸出者は、個人データの処理(個人データの移転自体を含む)を、該当するデータ保護法に従い実施してきたこと、また、今後も引き続き上記法令に従いこれを実施すること(また、該当する場合には、データ輸出者が設立されたEU加盟国の関係当局に通知を行っていること)、さらに、当該加盟国の関連条項に違反しないこと。
- (b) データ輸入者に対し、移転された個人データの処理を、適用データ保護法及び本契約条項に従い、当該データ輸出者のためにのみ行うよう指示していること、また、個人データ処理サービスの継続期間を通じて、かかる指示を行うこと。
- (c) データ輸入者が、付属書類2で特定される技術的及び組織的セキュリティ対策に関して、十分な保証を与えること。
- (d) 該当するデータ保護法要件の評価に従い、セキュリティ対策が、特にネットワークを通じた送信による処理が行われる場合の偶発的又は違法な破壊、偶発的な喪失、変更、不正開示又はアクセス、及びその他のあらゆる違法な処理形態から個人データを保護するのに適切なものであり、また、これらの対策が、最新の技術と対策実施費用を考慮した上で、処理及びデータの本質により生じるリスクを回避できるよう適切なレベルのセキュリティを確保するものであること。
- (e) セキュリティ対策の確実な遵守を図ること。
- (f) 当該移転に特別カテゴリーのデータが含まれる場合、データ主体に対し当該データ主体のデータが Directive 95/46/EC の意義の範囲で十分な保護が提供されていない第三国に移転される可能性がある旨を通知済みであること、もしくは事前に通知すること、又は事後的に可能な限りすみやかに通知すること。
- (g) 第5条(b)項及び第8条(3)項に基づきデータ輸入者又は復処理者から受領した通知を、データ保護監督当局に転送すること。ただし、データ輸出者が、移転の継続又は移転の一時停止を解除する旨を決定した場合に限る。
- (h) 要請に応じ、データ主体に対し、本契約条項のコピー1部(ただし、付属書類2は例外とする)及びセキュリティ対策の概要、並びに復処理サービスに関する契約書(この契約は、本契約条項に従い作成されなければならない)のコピー1部を提供すること。ただし、本契約条項又は復処理サービス契約に商業上の情報が含まれる場合、データ輸出者は、当該商業上の情報を除外することができる。
- (i) 復処理が行われる場合、当該処理業務が、データ主体の個人データ及び権利に対し、少なくとも本契約条項におけるデータ輸入者と同レベルの保護を提供する復処理者により、第11条に整合的に実施されること。
- (j) 第4条(a)項～(i)項の遵守を確保すること。

### 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、以下を保証する。

- (a) 個人データの処理を、データ輸出者のためにのみ、データ輸出者の指示及び本契約条項に従って行うこと。何らかの理由により上記を遵守することができない場合、データ輸入者は、すみやかにデータ輸出者に通知することに同意する。この場合、データ輸出者は、データ移転を一時停止する権利及び/又は本契約を解除する権利を有する。
- (b) データ輸入者に適用される法令により、データ輸出者からの指示の遂行及び本契約に基づく自身の義務の履行が妨げられると信じる理由は存在しないこと。また、本契約条項に規定された保証及び義務に実質的に悪影響を及ぼすおそれのある上記法令への変更が行われた場合、

データ輸入者は、当該変更を認識した後すみやかに、データ輸出者に対して当該変更を通知すること。この場合、当該データ輸出者は、データ移転を一時停止する権利及び/又は本契約を解除する権利を有する。

- (c) 移転された個人データの処理を行う前に、付属書類 2 で特定される技術的かつ組織的セキュリティ対策を講じていること。
- (d) 以下について、データ輸出者にすみやかに通知すること。
  - (i) 法執行機関から、法的拘束力を有する個人データの開示要請を受けた場合。ただし、通知を行うことが禁止されている場合 (たとえば、刑法に基づく法執行機関の捜査の機密性を維持するための禁止) を除く。
  - (ii) 偶発的又は不正アクセス。
  - (iii) データ主体から直接受けた要請 (通知以前に要請への対応を行わない)。ただし、対応することが認められている場合を除く。
- (e) 移転の対象である個人データの処理に関するデータ輸出者からの全ての質問を、迅速かつ適切に処理すること。また、移転されたデータの処理に関する監督当局からの助言に従うこと。
- (f) データ輸出者の要請に応じ、データ輸出者又は検査機関 (監督当局との合意により (該当する場合)、データ輸出者により選定された、独立性及び必要とされる専門的資格を有し、機密保持義務に拘束されるメンバーにより構成される) が実施する、本契約条項の対象となる処理活動の監査のためにデータ処理設備を提供すること。
- (g) 要請に応じ、データ主体に対し、本契約条項又はデータの復処理に関する既存の契約書のコピー 1 部を提供すること (ただし、本契約条項又は上記復処理契約に商業上の情報が含まれる場合は、当該商業上の情報を除外することができる)。ただし、付属書類 2 については、データ主体がそのコピーをデータ輸出者から入手できない場合は、セキュリティ対策の概要で代替するものとする。
- (h) データの復処理が行われる場合、事前にデータ輸出者に通知し、事前の書面による同意を取得していること。
- (i) 復処理者による処理サービスが、本契約条項の第 11 条に従い実施されること。
- (j) 本契約条項に基づき締結されたデータの復処理契約書のコピー 1 部をすみやかにデータ輸出者に送付すること。

## 第 6 条

### 法的責任

1. 両当事者は、当事者のいずれか又は復処理者が本契約条項の第 3 条又は第 11 条に違反したことにより損害を被ったデータ主体が、当該損害について、データ輸出者から賠償を受ける権利を有することに同意する。
2. データ輸出者が事実上消滅し、もしくは法律上存在しなくなったこと、又は支払不能に陥ったことのために、データ主体が、データ輸入者又は復処理者が第 3 条又は第 11 条に基づく義務に違反したことに起因する第 1 項に基づく賠償請求をデータ輸出者に対して行うことができない場合、データ輸入者は、データ主体が、あたかもデータ輸入者がデータ輸出者であるかのように、データ輸入者に対して請求を行うことができることに同意する。ただし、データ輸出者の承継人が、契約又は法律により、データ輸出者の法的義務を全て引き受けた場合を除く。この場合、当該データ主体は、当該承継人に対して権利を行使することができる。  
データ輸入者は、復処理者により違反が行われたという事実によって自身に法的責任を回避することはできない。
3. データ輸出者及びデータ輸入者の双方が事実上消滅し、もしくは法律上存在しなくなった場合、又はこれらの双方が支払不能に陥ったために、データ主体が、復処理者が第 3 条又は第 11 条に規定された義務に違反したことに起因する請求について、第 1 項及び第 2 項に規定されたデータ輸出者又はデータ輸入者に対する請求を行うことができない場合、復処理者は、データ主体が、本契約条項に基づく復処理者の復処理に関して、あたかも復処理者がデータ輸出者又はデータ輸入者であるかのように、復処理者に対して請求を行うことができることに同意する。ただし、データ輸出者又はデータ輸入者の承継人が、契約又は法律により、データ輸出者又はデータ輸入者の法的義務を全て引き受けた場合を除く。この場合、データ主体は、当該承継人に対して自身の権利を行使することができる。復処理者の法的責任は、本契約条項に基づく自身の処理業務に限定されるものとする。

## 第 7 条

### 調停及び裁判管轄

1. データ輸入者は、データ主体が本契約条項に基づきデータ輸入者に対して第三受益者としての権利を行使し、及び/又は損害賠償請求を行った場合、データ主体による以下の決定に従うことに同意する。
  - (a) 当該紛争を、独立の第三者、又は監督当局 (該当する場合) による調停に付託すること。
  - (b) 当該紛争を、データ輸出者が設立された EU 加盟国の裁判所に付託すること。
2. 両当事者は、データ主体が上記選択を行っても、データ主体が国内法又は国際法の他の条項に従い救済を求める実体的権利又は手続的権利に影響を与えないことに同意する。

## 第8条

### 監督当局との協力

1. データ輸出者は、監督当局が要請した場合、又は該当するデータ保護法に基づき必要とされる場合、本契約書のコピー (1部) を監督当局に預けることに同意する。
2. 両当事者は、監督当局がデータ輸入者及び復処理者の監査 (該当するデータ保護法に基づくデータ輸出者に対する監査と同じ範囲の監査であり、上記監査に適用される条件と同一の条件に服する) を行う権利を有することに同意する。
3. データ輸入者は、第2項に基づくデータ輸入者又は復処理者の監査の実施を妨げる、データ輸入者又は復処理者に適用される法律が存在する場合に、データ輸出者にすみやかに通知するものとする。この場合、データ輸出者は、第5条 (b) 項で想定される措置を講じる権利を有するものとする。

## 第9条

### 準拠法

本契約条項は、データ輸出者が拠点を置く EU 加盟国の法律に準拠するものとする。

## 第10条

### 本契約の変更

両当事者は、本契約の変更又は修正を行わないことを約束する。ただし、両当事者が、本契約条項と矛盾しない限度で、必要に応じて商取引上の条項を追加することは妨げられない。

## 第11条

### 復処理

1. データ輸入者は、データ輸出者の事前の書面による同意を除外し、本契約条項に基づきデータ輸入者がデータ輸出者のために履行する処理業務を委託しないものとする。データ輸入者が、データ輸出者の同意を得て本契約条項に基づく自身の義務を委託する場合、データ輸入者は、本契約に基づきデータ輸入者に課されるものと同一の義務を復処理者に課す契約を書面で締結することによってのみ、かかる復処理の委託を行うものとする。1復処理者が、かかる書面による契約に基づくデータ保護義務の履行を怠った場合、データ輸入者は、当該契約に基づく復処理者の義務の履行について、データ輸出者に対し完全に責任を負うものとする。
2. データ輸出者又はデータ輸入者が事実上消滅し、もしくは法律上存在しなくなった場合、又はこれらの双方が支払不能に陥った場合で、かつ契約又は法律によりデータ輸出者又はデータ輸入者の法的義務を全て引き受ける承継人が存在しないため、データ主体が第6条1項に規定された損害賠償の請求をデータ輸出者又はデータ輸入者に対して行うことができない場合に備え、データ輸入者と復処理者との間の事前の書面による契約には、第3条に定められている第三受益者条項を規定するものとする。データ復処理者の第三者に対する法的責任は、本契約条項に基づく自身の処理業務に限定されるものとする。
3. 第1項で言及される、契約に基づく復処理におけるデータ保護の観点に関する規定は、データ輸出者が拠点を置く EU 加盟国の法律に準拠するものとする。
4. データ輸出者は、本契約に基づき締結され、第5条 (j) 項に基づきデータ輸入者から通知された復処理契約のリストを保管するものとする。同リストは、少なくとも1年に1回の更新が行われるものとする。同リストは、データ輸出者のデータ保護監督当局も入手することができるものとする。

## 第12条

### 個人データ処理サービス終了後の義務

1. 両当事者は、データ処理サービスの提供が終了した際、データ輸入者及び復処理者が、データ輸出者の選択に従い、移転された全ての個人データ及びそのコピーをデータ輸出者に返却するか、又は全ての個人データを破棄し、データ輸出者に対して破棄を行った旨を証明することに同意する。ただし、データ輸入者に適用される法律により、データ輸入者が移転されたデータのすべて又は一部の返還又は破棄することが防止されている場合を除く。この場合、データ輸入者は、移転された当該個人データの機密性を保証すること及び当該個人データの処理を積極的に行わないことを保証する。
2. データ輸入者及び復処理者は、データ輸出者及び/又は監督当局の要請に応じ、第1項に規定された措置の監査のため、データ処理設備を提供することに同意する。

**データ輸出者代表者**

氏名 (フルネーム):

役職:

住所:

本契約が拘束力を有するために必要なその他の情報 (存在する場合):

署名: .....

組織印

**データ輸入者代表者**

氏名 (フルネーム):

役職:

住所:

本契約が拘束力を有するために必要なその他の情報 (存在する場合):

署名: .....

組織印

## 標準契約条項の付属書類 1

本付属書類は、本契約条項の一部を構成する。両当事者は、本付属書類の全項目に必要事項を記入の上、これに署名しなければならない。

EU 加盟国は、国内における手続きに従い、本付属書類に含めるべき必要な追加情報を補完又は記載を行うものとする。

### データ輸出者

本件移転に関するデータ輸出者の活動は、以下のとおりである (以下の欄に簡潔に記載)

.....

### データ輸入者

本件移転に関するデータ輸出者の活動は、以下のとおりである (以下の欄に簡潔に記載)

.....

### データ主体

移転される個人データは、以下のカテゴリのデータ主体に関するものである (以下の欄に具体的に記載)

.....

### データのカテゴリ

移転される個人データは、以下のデータカテゴリに関するものである (以下の欄に明記)

.....

### 特別カテゴリのデータ (該当する場合)

移転される個人データは、以下のデータの特別カテゴリに関するものである (以下の欄に明記)

.....

### 処理業務

移転される個人データは、以下の基本的な処理活動の対象となる (以下の欄に明記)

.....

### データ輸出者

氏名: .....

正式な署名: .....

### データ輸入者

氏名: .....

正式な署名: .....

## 標準契約条項の付属書類 2

第 4 条 (d) 項及び第 5 条 (c) 項に従い、データ輸入者により講じられた技術的かつ組織的セキュリティ対策の説明 (又は文書/法律を添付):  
本合意の別紙 A を参照。