標準購入規約

別紙 A

Carrier 情報のセキュリティ

本方針の以下の規定は、売主が Carrier 情報を保管する場合はいつでも、https://www.corporate.carrier.com/suppliers/terms-conditions/に掲載されている Carrier の標準購入規約（以下「本規約」という。）及び本契約に組み込まれるものとする。本方針で使用されている大文字で始まる用語で定義されていないものはすべて、本規約で与えられたものと同じ意味を有するものとする。

1. 売主は、(*a*)売主のネットワーク、システム及び運営、本サービス及び Carrier 情報のセキュリティ、利用可能性及び完全性を保護し、(b)セキュリティ問題を防止し、(c)ISO 27001 の認証要件を満たすように設計された管理、技術及び物理的保護措置を策定、維持、遵守するために商業的に合理的な努力をする。売主は、Carrier 情報を不正なアクセス及び使用から保護するために設計された適切な管理、技術、組織及び物理的な保護措置、セキュリティ意識並びにセキュリティ対策を含む、本買主が合理的に受け入れ可能な書面によるセキュリティ・プログラムを開発、実施、維持する。

2.売主は、効果的な情報セキュリティを提供し、本買主が受け入れ可能なセキュリティ・ハードウェア、ソフトウェア、手順及び方針をインストールし、実装することに同意する。売主は、関連する情報及びセキュリティ・ソリューションの現状に適した水準のセキュリティ保護、準備、回復力を維持するために、改良された技術を利用し、進展するセキュリティ脅威に対応するためのハードウェア、ソフトウェア、手順、方針を監視し、更新することに同意する。要求に応じて、売主は、本契約及び／若しくは注文書の期間中に売主により若しくは売主に代わって行われた IT セキュリティに関連する内部監査の報告若しくは結果、又は SSAE16 レポート若しくは ISAE3402 に基づくものを含むがこれに限定されない監査報告書を本買主に提供するものとする。

3. 売主は、さらに以下のことに同意する。

3.1 本契約及び／又は注文書に基づく義務の履行において、本方針に定める規定を遵守して、又は法的義務を遵守するためにのみ、Carrier 情報を収集、これにアクセス、これを使用、共有し、又は許可された第三者に Carrier 情報を移転すること。売主は、(a)本規約に基づく本買主の本サービス購入に関連して本買主が書面で明示的に許可した場合、又は(b)法律により要求された場合を除き、Carrier 情報の二次的使用又はその他の使用（データマイニング目的など）を行うことはない。

3.2 少なくとも以下の領域に対応する情報セキュリティ方針を維持、実施すること。

3.2.1 情報セキュリティポリシー

3.2.2. 情報セキュリティの組織

3.2.3 資産管理

3.2.4 人的資源によるセキュリティ

3.2.5 物理的及び環境的セキュリティ

3.2.6 通信及び運用管理

3.2.7 アクセス制御

3.2.8 情報システムの取得、開発及び保守

3.2.9 情報セキュリティインシデント管理

3.2.10 事業継続管理

3.2.11 規制遵守

3.3 各領域が本条と一致する方法で対処されていることを本買主が合理的に満足できるように証明するのに十分な方針の索引又は類似の概要を本買主に提供すること。売主は、本買主の要求に応じて、最新の索引又は概要を本買主に提供し、方針を遵守するために計画されたアップグレードの実施予定表を含む計画を示すものとする。売主は、本買主が要求する当該方針の変更に関する合理的な要求を実施するものとする。

3.4 本買主又はその被指名人が 1 日前に通知することにより、その施設においてセキュリティ監査を実施すること、及び本買主がいつでもネットワーク監査を実施する（又は実施させる）ことを許可すること。本買主の同意に基づき Carrier 情報が共有環境に保管されている場合、本買主は、当該監査を実施するために第三者を利用するものとする。監査には、バックアップ保管施設を含む Carrier 情報を有するすべての施設が含まれるものとする。

3.5 本買主の別段の同意がある場合を除き、すべての Carrier 情報を、本買主、並びにその代理人及び本サービスを履行するため、又は機器及び機器が動作するプログラムを保守するためにアクセスを必要とする売主の従業員及び代理人のみがアクセスできる別のデータベースに分離すること。本買主が承認する場合、データの論理的な分離は、本要件の代わりとして認められることがある。売主は、その時点で利用可能な技術によって測定される合理的な努力をし、その権限を与えられた従業員、本買主及びその代理人以外が Carrier 情報にアクセスするのを防止するものとする。

3.6 すべての Carrier 情報及び該当するソフトウェアが適切にバックアップされ、災害又は緊急事態が発生した場合に復旧可能であること、及び売主の災害復旧計画（本規約において別途要求される場合がある。）にかかる要件が組み込まれていることを保証すること。

3.7 本契約及び／又は注文書の署名時に、本契約及び／又は注文書の終了時に Carrier 情報を本買主に返却する方法（バックアップ及びアーカイブ情報を含む。）、並びにすべての Carrier 情報を売主の機器及び施設から恒久的に除去する方法を記載した終了計画を本買主に提供すること。この計画には、業界で認められた非専有データベースで本買主にデータを提供すること、そうでない場合は、データにアクセスするための専有データベース・ソフトウェアを使用するライセンスを含める必要がある。

3.8 Carrier 情報を求める召喚状、調査などに応じて本買主に情報を提供し、全面的に協力し、売主の保有する情報を含むその情報に関して、本買主が証明などを求めるための情報及び支援を提供すること。売主は、Carrier 情報を第三者に提供することを求める要求を受けた場合、速やかに本買主に通知するものとする。

3.9 本買主が要求する場合、売主は、本買主から売主に提供された Carrier 情報セキュリティ方針を合理的な期間内に遵守することに同意する。

3.10 売主は、本買主の書面による事前承認なしに、他の事業体に Carrier 情報を提供しないものとする。本買主の承認の要求には、(i)本規定のすべての要件がその履行に適用されること、及び(ii)本買主が上記の監査を実施する権利を有することへの売主及び当該他の事業者による同意が含まれるものとする。

4. 暗号化要件　売主は、本契約及び／又は注文書に基づき承認又は許可される Carrier 情報の移転、通信、リモートアクセス又は保存（バックアップ保存を含む。）に関連するものを含む、Carrier 情報の処理に関して、常に適切な形式の暗号化又はその他の安全技術を使用し、売主の人員に使用させる。本規約のこれと異なる定めにかかわらず、本買主の個人情報は、売主のモバイルコンピューティング機器（ラップトップコンピュータ、PDA（携帯情報端末）など）に保存しないものとする。

5. 通知　売主は、(i)情報セキュリティに関するその時点の基準を満たさない場合、並びに(ii)合理的に疑われる、及び／又は確認されたすべてのセキュリティ問題について、本買主に直ちに書面で通知する。当該通知は、当該セキュリティ問題により影響を受ける本買主又は個人への影響、並びに売主が実施又は提案する是正措置及び改善努力を合理的な範囲で詳細に要約する。売主又は本買主のいずれが特定したかにかかわらず、セキュリティ問題が生じた場合又はその他情報セキュリティの基準を満たさない場合直ちに、売主は、もたらされるリスクを軽減するための措置を講じ、改善努力について本買主と誠実に協議し、本買主がその単独かつ合理的な裁量で、セキュリティ問題若しくは不履行の性質に見合った状況において必要、合理的若しくは適切であると判断する、又は政府機関により要求される是正計画を実施する。売主は、セキュリティ問題が是正されたことを確認するために実施する再テストの合理的な費用を含むがこれに限定されない、すべての費用及び経費について単独で責任を負うものとする。本買主が指定する期間内及び方法でセキュリティ問題又は不履行のリスクを是正しない場合、本方針、本規約及び／又は本契約の重大な違反とみなされる。

