情報セキュリティプラン

BPCS/LX, XA, System 21

適用範囲：本情報セキュリティプラン（以下、「ISP」という）は、Inforと締結された顧客の契約（以下、総称して「当該契約」という）に組み込まれる。本ISPの条件と当該契約の条件に矛盾または不一致が生じた場合には、本ISPを優先させる。本ISPをもって、以下を保護するために策定されたInforの現行のセキュリティ対策を定めるものとする。

(i) Inforが以下を提供するためのハードウェア、機器、及びシステム・ソフトウェア・コンフィギュレーション：
- クラウドサービス（明確にするために付記すると、クラウドサービスにはサポートが含まれる）；
- プロフェッショナルサービス：及び
- オンプレミスソフトウェアに対するサポート

（本 ISP においては、以下、これらすべてのハードウェア、機器、及びシステム・ソフトウェア・コンフィギュレーションを総称して「当該システム」といい、また、本 IPS においては、以下、クラウドサービス、プロフェッショナルサービス、及びオンプレミスソフトウェアのサポートを総称して「当該サービス」という）：また、

(ii) 以下のいずれかの顧客データ：
- 顧客データとしてInforに提供されるもの；または
- プロフェッショナルサービス、及び／またはInforの環境から行うサポートを実施するために、Inforに提供されるもの

（本ISPにおいては、以下、すべてのこのようなデータを総称して「当該データ」という）。

定義：本ISPにおいて使用される用語で、本ISPにおいて定義されていないものは、Infor及び当該顧客間のソフトウェア契約（以下、「当該ソフトウェア契約」という）の用語と同義である。

除外事項：本ISPは、以下には適用されないものとする。：（i）別途取り決められたプロフェッショナルサービスの契約に基づいて、Inforによりホストされている顧客のオンプレミスソフトウェアに対するInforプロフェッショナルサービスのアレンジメント、または（ii）Inforが、顧客のサイトにおいて、及び／または顧客のシステムへのアクセスを提供されて、サービスを実施する場合。それらの場合、Inforは、サービス個別契約において双方が同意した、顧客の管理条件、並びに技術的及び物理的条件を遵守するものとし、顧客のシステムへのアクセスに関しては、顧客は、顧客が適切であると判断するところにより、顧客のシステムにアクセスするためのユーザー認定及びパスワードをInforの従業員に提供すること、及びかかる認定の取り消し及びアクセスの解除に責任を負うものとする。

アップデート：セキュリティ上の脅威、及びそうしたセキュリティ上の脅威から保護するために策定される対策は、絶えず進化しているため、Inforは、本ISPを、顧客に通知することなく、いつでも変更できるものとするが、ただし、Inforは、当該システム及び当該データについて、総合的に、同等またはより高いセキュリティレベルを維持するものとする。

1. 一般セキュリティ標準

Inforは、当該システム及び当該データを破壊、損失、不正アクセスまたは改変から保護する目的で策定された、管理上、並びに技術的及び物理的安全対策を保持するが、それは：（i） Inforが自身の同種の情報を保持する以上の厳格性を有し；（ii）一般的に容認された業界標準以上の厳格性を有し；かつ（iii）適用法の要件を満たすものでなければならない。

1.1 セキュリティ担当者

Inforは、本ISP上のセキュリティ対策を調整及び監視する責任を負う、1名以上のセキュリティ管理者を選任している。

1.2 アクセスコントロール

Inforは、当該データについて、以下の対策を含むが、それに限定されないアクセスコントロールを実施する。

i. Inforは、当該データにコンピュータからアクセスする各人に固有のIDを割り当てる。

ii. Inforは、当該データへのアクセスを付与、変更または解除できる従業員を特定し、当該データへのアクセス権限を最小限に制限する。当該データへのアクセスは、サービスを提供するために「知る必要のある」従業員にのみが許可するものとし、Inforはかかる従業員の記録を保持し、更新する。また、こうしたアクセスはログが録られ、監視されるものとする。

iii. Inforは、当該データへのアクセスを有するInforの従業員に対し、コンピュータの前から離れる時には、業務セッションを無効化するよう指導する。

iv. Inforは、Inforの従業員が退職または異動する場合、もしくは彼らが当該データへのアクセスを必要としなくなった場合には、当該データが含まれるアプリケーションまたはデータストアから、当該従業員のアカウントを無効にする。Inforは、当該データにアクセスする者及びサービスのリストを定期的に確認し、アクセスが必要なくなったアカウントは削除する。Inforは、この確認を少なくとも半年毎に行うものとする。

v. Inforは、いかなる当該システムにおいても、パスワード及びその他のセキュリティパラメータに、製造者が設定した初期設定のものを使用しない。Inforは、すべてのInforの当該システムについて、一般的に容認されている業界のベストプラクティスに準じた、システム-エンフォースされた「強固なパスワード」の使用を義務づけている。Inforは、すべてのパスワード及びアクセス認証を機密として保持し、従業員間でシェアしないよう求め、不正や開示があったことを知り得たパスワードは無効にする。

vi. Inforは、アカウントに誤ったパスワードが指定回数を超えて連続して入力された場合には、当該データへのアクセスを有するアカウントを無効化することによって「アカウント・ロックアウト」状態にする。

vii. 当該データが納められた当該システムへのリモートアクセスには、二要素認証（例：ユーザーを特定するのに、少なくとも2つの異なる要素が要求される）が必要とされる。

1.3 侵入の検知及び防止

Inforは、セキュリティ侵害、違反及び疑わしいアクティビティがないか、当該システム及びそのプロセスを監視するのに、侵入検知システム／侵入防止システム（IDS／IPS）を使用する。これには、疑わしい外的アクティビティ（不正な探査、スキャンまたは侵入の試みを含むがそれに限定されない）及び疑わしい内的アクティビティ（不正なシステム管理者アクセス、当該システムの不正な変更、当該システムの不正利用または盗用、もしくは当該データの誤使用を含むがそれに限定されない）が含まれる。Inforは、悪質な行為や不正アクセスの兆候がないか、定期的にアクセスログを確認する。

1.4 ファイアウォール

Inforは、インターネットからアクセス可能な当該データを保護するために設計されたネットワークファイアウォール技術を保持する。

1.5 アップデート

Inforは、アップグレード、アップデート、バグフィックス及び新バージョンをもって当該システムを最新の状態に保つ。オペレーティングシステム及びアプリケーションシステムのアップデート／アップグレード／修正は、顧客と共に準備し、予定を組むものとする。

1.6 データの暗号化

i. 公共ネットワークへの送信中、当該データは、最低限TLS1.2またはその論理的後継によって暗号化される。

ii. 当該データが当該システム内にある間は、クラウドサービスについては、当該データは、最低限AES 256ビットまたはその論理的後継によって暗号化される。

1.7 ID管理

Inforは、ID管理の責任を分配する共有型セキュリティモデルを活用する。Inforは、認証のために、当該システム内のアプリケーションを顧客のID管理プロバイダに戻って連携させることができる。

1.8 物理的セキュリティ

当該システムが設置される施設においては、以下の事項を順守する。

i. 厳しい気候条件や、その他の合理的に予測可能な自然条件に、耐え得るような構造で設計されていること；
ii. 煙、熱、水、火、湿気、または電力の不安定から当該システムを保護できるように、物理的環境において適切な防止策を講じていること；
iii. 現地のバックアップ電力供給システムによってサポートされていること；かつ
iv. 認証された従業員のみが、施設への物理的なアクセスを許可されることを徹底するよう策定された適切なコントロールがなされていること。

2. 監査

2.1 監査権

ベンダー監督プログラムの一環として、顧客及び（該当する場合には）政府の監督機関は、情報セキュリティに関するプログラム、プロセス及びコントロールに関するInforからの手続き書類（例：ISO27001に基づくアンケート）を、1年に1回郵送による監査という形式で請求することができる。Inforは、かかる手続き書類が容易に取得できる範囲で同意し、Inforは、顧客が合理的に請求する書類を、以下に該当する限りにおいて提供する。：（a）かかる書類が、Inforのその他の顧客のデータもしくはサービスの機密性、整合性、または利用可能度を脅かさないこと；また、（b）かかる書類が、Inforを代理して顧客に当該サービスを提供する第三者のデータもしくはサービスの機密性、整合性及び利用可能度を侵害しないこと。Inforが提供する手続き書類には、証明書類（例として、研修の証明、テストの証明、リスク評価の結果などがあるが、それに限定されない）は含まれない。Inforは、30日以内にアンケートに回答する。この期限内の回答が不可能である場合、Inforは顧客と協力して、手続きの完了までの合理的なスケジュールが双方の合意に達するよう努める。かかるすべての書類は、Inforの機密情報とする。Inforは、本郵送による監査の結果生じる顧客の所見について考慮しない。

2.2 第三者による監査

サブスクリプション期間の12ヶ月毎に1回、Inforは、自らの費用負担で、正規の資格を有する独立監査人に依頼して、クラウドサービス（サポートは含まない）に関係する、Inforが定義したコントロール目標及びコントロール作業の策定及び運用の有効性の調査を実施しなければならない。Inforは、かかる監査人に、すべてのクラウドサービスについてはSOC I タイプ2の報告書を、マルチテナント型クラウドサービスに限っては、SOC II タイプ２の報告書（以下、総称して、「監査報告書」という）を用意させるものとする。当該監査報告書は、Inforの機密情報であるが、顧客はInforのサポートポータル上で利用できる。顧客は、かかる監査報告書の写しを監査人及び監督機関と共有することができる。ただし、それにはその監査人及び監督機関が、かかる監査報告書がInforの機密情報であり、相応の保護が必要であることを通知されていることを条件とする。

3. クラウドサービスの変更管理

Inforは、Inforのクラウドサービスを提供するリソース内の変更について、その特定及び実施を規定する変更管理プロセスに従うことにより、アプリケーション・ソースコード、インターフェース、オペレーティングシステムまたは既存のフィールド及びテーブル内のデータのバックエンド変更について、望ましくない変更の防止に役立てる。Inforのサクラウドサービスを提供するリソースに対するすべての変更依頼は、変更管理プロセスに従って実施するものとする。Inforは、チケッティングシステムや、変更の日付と時刻並びに変更タイプの説明を含むがそれに限定されない、あらゆる変更に関するテスト工程の記録等の、本プロセスの遵守に関する詳細な記録を文書化して保持する。

4. 当該データの分離; 利用の禁止

4.1 分離

当該データは、Inforのデータ及び他のInfor顧客のデータから、適切な技術的方法により、論理的に分離された状態が保たれ

る。

4.2 不使用; 蓄積された統計情報

当該データは、顧客の機密情報であり、顧客は自身の当該データに対して全面的な所有権を有する。Inforは、当該サービスの実施、または当該ソフトウェア契約に基づく自らの義務の履行に必要である場合を除き、当該データを商業的に利用せず、当該データにアクセスしないものとする。

当該データに関し、Inforは、蓄積された統計情報を収集する権利を有するものとし、その情報は、Infor単独の所有物であり、顧客データとはみなされない。「蓄積された統計情報」とは、計測及びログ記録システムを通じて生成された、顧客による当該サービスの利用及び運用に関する統計データ及びパフォーマンス情報である。

5. 資産管理

Inforは、正式な資産管理プロセスを持ち、それには以下を保持することが含まれる。

i. 資産の明確な所有権及び支配権を特定し、確立できるように策定された、当該サービスの提供のために使用される資産インベントリ（以下、「資産」という）；
ii. 該当する資産からの当該データの返却、破棄、または削除の管理のために策定されたプロセス；及び
iii. 内的か外的か、故意か偶発的かに関わらず、資産を脅威及び脆弱性から保護するために策定されたプロセス。

6. 脆弱性のスキャニング及び侵入テスト

Inforは、公開または特定された欠陥もしくは弱点を（偶発的か意図的かに関わらず）衝かれることにより生じ、結果として当該システムへの有害もしくは不正なアクセスを招く可能性のあるリスク（以下、「脆弱性」という）をスキャンするための、脆弱性管理プロセスを保持する。Inforは、一般的に容認されている業界標準の時間枠内で脆弱性に対処する。Inforは、一般的に容認されている業界標準と一致する、Inforが定義するフレームワークに従い、脆弱性がもたらすリスクに見合った方法で、脆弱性を改善または軽減する。

年次ベースで、Inforは、マルチテナント型クラウドサービスについて、当該システムのセキュリティコントロールを評価するために、自らの費用負担で、独立した第三者に依頼し、一般的に容認されている業界標準のメソッドに従って侵入テストを実施するが、それには人が手動で行うテストを含むものとする。

マルチテナント型クラウドサービスについて、ソースコードスキャンや脆弱性スキャンを含むセキュリティテスト評価は、潜在的な脆弱性を特定し、改善または軽減できるよう、コードのリリースの前、及びクラウドサービス製品のライフサイクル（例：開発環境及び本番環境）を通じて行われる。年次ベースの侵入テストは、改善または軽減すべき脆弱性を特定するため、マルチテナント型クラウドサービスにおいて実施される。

7. 情報セキュリティインシデント対応

Inforが、当該データについて、当該ソフトウェア契約で認められていない使用または開示の事実、または合理的にそう推測される状況（以下、「情報セキュリティインシデント」という）を認識した場合、Inforは、（i）速やかに、不当な遅滞なく（いかなる場合でも、かかる情報セキュリティインシデントを認識してから48時間以内に）顧客に対して、情報セキュリティインシデントの発生を通知し；（ii）調査の上、かかる情報セキュリティインシデントの原因について合理的な分析を行い；（iii）顧客に、進行中の調査に関して定期的に最新情報を提供し；（iv）かかる情報セキュリティインシデントの原因を、Inforがコントロールできる範囲において改善するための、適切なプランを策定、実施し；そして（v）かかる情報セキュリティインシデントに適用され得る、あらゆる通知またはその他規制上の要求に応じるため、顧客の合理的な調査または顧客の努力に協力しなければならない。顧客の要請に応じて、顧客の費用負担において、情報セキュリティインシデントが発生した際、Inforは顧客に対し、（法律により認められる限りにおいて、適切な機密保持を条件として）該当するシステム・アクティビティの記録の写し（ただし、顧客に関連する情報セキュリティインシデントに関する内容に限る）を、顧客の法的もしくは規制上の手続き、または政府による調査において顧客が使用できるよう提供する。

8. ログの記録及び監視

Inforは、特にログ及びアラートの管理を目的として設計された一連のツールを使用して、当該サービスを提供するために使用される自らのリソースを監視する。ログ記録は、改ざんを防止できるよう、物理的かつバーチャルに安全に保管される。機密性の高い情報及びパスワードは、いかなる状況においても記録されない。当該サービス関連情報の捕捉に加え、監視ツールによって、管理者は、ユーザーが当該システムにログイン及びログアウトする際のアクティビティを追跡できる。

9. 人事的セキュリティ及びトレーニング

当該サービスを提供しているInfor従業員は、機密保持義務を負い、情報セキュリティの脅威及び懸念に関する知識を有し、少なくとも年次ベースで一般的なセキュリティトレーニングを受講するとともに、組織的な情報セキュリティポリシーを、自身の担当部門においてだけでなく全体としてもサポートできるよう備えている。

10. エンドポイントデバイスコントロール（Inforのラップトップ、ワークステーション及びモバイルデバイス）

Inforは、アプリケーション及びオペレーティングシステムのパッチ管理の自動化並びにウイルス対策保護を含む、エンドポイントの保護のため、一般的に容認されている業界標準に則ったセキュリティ対策を実装している。

11. データの返却及び破棄

11.1 返却

クラウドサービスの終了または満了をもって、Inforは、速やかに（標準的なサポートチケットの提出による、顧客の書面での要請を受領してから3～5営業日以内とする）すべての顧客データを、Inforの安全なファイルトランスファーサービスを通じて提供されるネイティブデータベースエクスポートにより、顧客が利用可能な状態にする。顧客が、当該データの代替形式による返却を希望する場合、または、その他の終了支援サービスを希望する場合には、Infor及び顧客は、かかる終了支援サービスの範囲、かかる終了サービスに対して支払われるべき料金及び経費について相互に合意するものとする。終了する前に、顧客は、アプリケーションインターフェースから顧客データにアクセスすることができるものとし、Inforは、サポートポータルからの顧客の要求に応じて、、データバックアップのコピーを返却するものとするが、ただし、それはInforの安全なファイルトランスファーサービスを通じて提供されるネイティブデータベースエクスポートとして、12ヶ月に2回までとする。追加の要求には料金が発生するものとする。

更に明確にするために付記すると、個人情報の返却または破棄は、データ保護契約の条件に従うものとする。

11.2 破棄

顧客が移行アシスタンスを要求しない限り、Inforは、顧客データの（オンラインまたはネットワーク上のアクセス可能な）すべてのインスタンスを、NIST 800-88に従って、クラウドサービスの終了または満了より35日以内に、完全に削除するものとする。

サポートを実施する目的でInforに提供されたデータ（例：サポートポータルにログしたサポートチケットを通じて提供されたもの）は、インシデントチケットのクローズ日より5年間でパージされる。サポートチケットのライフサイクルの管理のために使用された顧客の個人の氏名及び担当者情報（例：ユーザー電子メールアドレス、氏名、及び電話番号）は、サポートの終了をもって、無効化及び匿名化される。

12. サブコントラクター

Inforの当該サービスに関連して、商品及びサービスをInforに提供しているInforのサブコントラクターは、かかる商品及びサービスを、本ISPで定める条件と実質的に同等の条件で提供する。Inforは、本書に基づく当該サービスを実施する目的で、第三者サブコントラクターと提携する前に、かかるサブコントラクターが本書で定める機密性及びセキュリティの義務を遵守できることを確認するため、合理的なディリジェンスをもってかかるサブコントラクターを調査する。Inforは、サブコントラクターが、当該サービスをサポートする中で為したすべての行為に責任を負う。