株式会社 NTT ExC パートナー

安全管理措置等チェックシート	7.1 版

貴社で取扱う情報を全て〇で囲んでください。	①特定個人情報（マイナンバー等）	②個人情報（特定個人情報を除く）	③財産的情報（個人情報・特定個人情報を除く）

注：財産的情報とは個人情報、システム情報、提案書、契約書等が該当します。

記入年月日	
貴社名	
部署名	
お名前 責任者	印
連絡先	

※本シート返送時のメール本文を、押印の代替とすることも可能です。

【目的】

この調査は弊社が個人情報（特定個人情報を含む）・財産的情報の授受が発生する場合に、契約またはサービス利用申込みを行う法人等ごとに、情報セキュリティ、個人情報保護（特定個人情報等を含む）の管理体制を確認させていただくものです。契約の形態を問わず、クラウドや Web サービス等の利用・共同利用・第三者提供についても対象です。

「個人番号」「特定個人情報」は、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下「番号法」といいます）で定義されています。

契約の締結またはサービス利用申込みにあたり、お手数ですが以下のチェック項目についてご回答願います。

〔回答項目〕

・『①特定個人情報（マイナンバー等)』の場合：全ページ（No.1-1～No.11-18）

・『②個人情報』『③財産的情報』の場合：P.1～3（No.1-1～No.7-12）

〔回答記号〕・・・　〇：はい、×：いいえ、－：該当しない

【情報保護に関する認証取得状況】

No	チェック項目	回答欄	回答欄追記欄
1-1	ISMS 認証※1 を取得している。 取得予定がある場合は予定日、更新済の場合は更新日をご記入願います。		最新取得年月日： 認証登録番号　： 適用範囲　：
1-2	プライバシーマークを取得している。 取得予定がある場合は予定日、更新済の場合は更新日をご記入願います。		最新取得年月日： 許諾番号　：
1-3	その他、情報保護に関する認証を取得している。 取得予定がある場合は予定日、更新済の場合は更新日をご記入願います。		認証名　： 最新取得年月日： 許諾番号　：

※1　ISMS 認証を事業部・部・課・プロジェクト等の単位で取得されている場合、当該業務が認証の範囲であるかを確認します。
全社で認証取得されている場合は、回答欄追記欄の『適用範囲』に「全社で認証取得」とご記入願います。

No	チェック項目	回答欄	記事欄
2-1	NTT グループ協定※2 の締結対象法人等である。 ※2「社員等個人情報の取り扱いに関する協定」 NTT グループではない場合は「－」をご記入願います。	－	
2-2	取り扱う個人情報が「NTT グループ協定」が定義した社員等個人情報である。 NTT グループではない場合は「－」をご記入願います。	－	

次ページ以降についてもご回答願います。

安全管理措置等チェックシート	7.1 版

■個人情報・財産的情報を取扱う場合■

No	チェック項目	回答欄		記事欄
		個人情報	財産的情報	“×”の場合の対策・実施予定時期
3-1	「個人情報保護方針」またはこれに準じるセキュリティポリシーを定め、公開している。			
	【組織的安全管理措置】			
4-1	個人情報保護、財産的情報保護の組織体制を定め、運用している。	—		
4-2	個人情報保護、財産的情報保護の社内規定を整備し、運用している。	—		
4-3	安全管理措置の評価及び見直し・改善を年１回以上、実施している。			
4-4	（事故等が発生した場合）調査報告書・再発防止策の作成、及び再発防止策の実施を義務づけている。			
4-5	貴社が業務の一部を第三者に委託する場合は、当該第三者に本調査と同様の調査を実施している。			
4-6	記録媒体や紙を廃棄する際、破壊・裁断等の処置を施している。また、外部に委託する場合は廃棄の証明書を取得している。			
	【人的安全管理措置】			
5-1	貴社と業務に携わる担当者の間で機密情報（個人情報を含む）の保持に関する同意書・誓約書等を取り交わしている。			
5-2	個人情報保護、財産的情報保護に関する教育を年１回以上、実施している。	—		
5-3	業務に携わる担当者全員に対し、当該業務が情報資産の取扱い業務であり、契約および社内規定に従い業務にあたるよう意識づけができており、担当者は皆取扱いルールを理解している。			
	【物理的安全管理措置】			
6-1	貴社の建物・施設・室には許可された者のみが入退できるようになっている。また、その記録を保管している。			
6-2	離席時に重要書類、記録媒体等を机上に放置させていない。また、ノートパソコンについては退社時等、長時間離席する場合、放置させていない。			
6-3	離席時にパスワード付スクリーンセイバー等を起動させている。			
6-4	業務で取扱う情報について、紙及び記録媒体は施錠保管している。			
6-5	取り扱う情報は国内に保管している。（情報を保管しているサーバ/クラウドは国内にある。）		—	“×”の場合　国名又は地域名：
6-6	業務の運用は国内で対応している。（運用を外国に委託していない。また運用のために外国から国内サーバ/クラウドへのアクセスを許可していない。）		—	“×”の場合　国名又は地域名：

安全管理措置等チェックシート	7.1 版

No	チェック項目	回答欄	記事欄 “×”の場合の対策・実施予定時期
	【技術的安全管理措置】		
7-1	業務で取扱う情報機器へアクセスする場合、ID とパスワードによる認証を実施している。		
7-2	上記情報機器及びデータへのアクセス権限は業務に携わる担当者に限定、かつ必要最小限の権限を付与している。		
7-3	アクセス権限を設定する管理者を限定している。		
7-4	アクセス記録の取得・保存、及び定期的な分析・監視を実施している。		
7-5	情報機器にウイルス対策ソフトを導入し、定期的なウイルスチェックを実施している。		
7-6	情報を移送・送信する際、当該データの暗号化またはパスワードによる保護を実施している。		
7-7	インターネット、無線 LAN 等のネットワークで個人情報を利用する場合、当該データの暗号化を実施している。		
7-8	情報システムの導入・変更にあたり、試験の実施とその結果を保管している。		
7-9	情報システムを監視または監査している。		
7-10	外部ネットワークからの不正侵入に対する適切な防御策（ファイアウォール、認証システム等を設置等）を講じている。		
7-11	情報機器の脆弱性対策（パッチの適用やバージョンアップ）を講じている。		
7-12	外部へ情報を持ち出せないよう、社内 PC から Web メールや外部ストレージ等へのアクセスを規制している。		

以上

取扱う情報が、『②個人情報』『③財産的情報』の場合は No.1-1～No.2-2、及び No.3-1～No.7-12 で確認終了です。
『①特定個人情報（マイナンバー等）』の場合は No.8-1～No.11-18 もご回答ください。