**【様式CS－3】**

|  |  |  |  |
| --- | --- | --- | --- |
| 20yy年mm月dd日  **CS言明書**  （会社名　　　　　　　　　　）  （役職　　　　　　　　　　　）  （氏名（署名または記名押印））  当社は、下記クラウドコンピューティングサービスを提供するにあたり、「クラウド情報セキュリティ基本言明要件」（「クラウド情報セキュリティ管理基準」）の求めるところに従い、情報セキュリティガバナンスのもとで情報セキュリティマネジメントを実施し、基本リスクに対する管理策を整備、実装、運用しています。  1.クラウドコンピューティングサービス名称   |  | | --- | |  |   2.対象範囲   |  | | --- | |  |   3.対象リスク   |  | | --- | |  | |

※1　申請時にCSマークの添付は不要です。

|  |  |  |
| --- | --- | --- |
| 4.詳細言明   |  | | --- | |  |  * 対象リスクに対応する詳細言明を記入例4.詳細言明の（1）～（4）から選んで 記入してください。   5.特記事項   |  | | --- | |  | |
| 付1.　対象リスク（詳細）  クラウド固有のリスク   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | （1）情報の漏えいリスクに関して（機密性） | | | | | | | 保護すべき情報が漏えいするリスク | | 利用者・サービス間の情報隔離に失敗する | | H05 | | | サービスエンジンの制御機能を奪われる | | H06 | | | クラウドプロバイダでの内部不正－特権の悪用 | | M07 | | | 管理用ユーザインターフェースに、不正にアクセスされ、使用、操作される | | M08 | | | データ転送途上における攻撃、データ漏えい  （アップロード時、ダウンロード時、クラウド間転送） | | M09 | | | 利用者別の情報削除、廃棄に失敗する | | M10 | | | サプライチェーン先から提供される業務が不全となる | | L14 | | | データの集中により当局によるデータ押収が行われた場合、他利用者含め情報が開示され、またサービスが停止する | | L18 | | | 国内外の法令等の開示、提出命令により、他利用者含め情報が開示され、またサービスが停止する | | L19 | | | （2）情報と処理の改ざんリスクに関して（完全性） | | | | | | 情報及び処理が改竄されるリスク  （情報及び処理が網羅されない、正確でないことを含む） | 利用者・サービスの高集約、共有化により、障害が派生、拡大する | | H01 | | | サービスエンジンの制御機能を奪われる | | H06 | | | クラウドプロバイダでの内部不正－特権の悪用 | | M07 | | | 管理用ユーザインターフェースに、不正にアクセスされ、使用、操作される | | M08 | | | サプライチェーン先から提供される業務が不全となる | | L14 | | | （3）サービス利用不能リスクに関して（可用性） | | | | | | サービス提供ができなくなるリスク  （利用者が利用したいときに、提供できないことを含む） | 利用者・サービスの高集約、共有化により、障害が派生、拡大する | | H01 | | | 物理／仮想環境の設計・設定・運用の不整合により、機能不全となる | | H02 | | | ある利用者・サービスの停止、抑止に伴い、他利用者がサービスを利用できなくなる | | H03 | | | リソースの事前準備、動的割当が不足し、増大する利用者需要に対応できない | | H04 | | | クラウド内DDos／Dos攻撃を受け、サービス不全となる | | M11 | | | 外部との相互運用性がなく、利用者のデータ移管、移行ができない（ロックイン） | | L12 | | | サプライチェーン先から提供される業務が不全となる | | L14 | |  |  |  |  | | --- | --- | --- | | （4）その他の情報セキュリティリスク | | | | セキュリティ要件  ／リスクカテゴリー | リスク要因 | | | 【機密性】  保護すべき情報が漏えいするリスク | 外部アクセス含め、アクセスコントロールが、有効に働かない | 他1 | | システム開発、保守、運用の管理の適切性が欠けている | 他2 | | 開発要員、保守要員、運用要員のオペレーションミス防止策が有効でない | 他4 | | ウイルス等不正プログラム対策が不備である | 他5 | | 【完全性】  情報及び処理が改竄されるリスク （情報及び処理が網羅されない、正確でないことを含む） | 外部アクセス含め、アクセスコントロールが、有効に働かない | 他1 | | システム開発、保守、運用の管理の適切性が欠けている | 他2 | | 災害、破壊行為により、設備・機器等のリソースが使用不能となる | 他3 | | 開発要員、保守要員、運用要員のオペレーションミス防止策が有効でない | 他4 | | ウイルス等不正プログラム対策が不備である | 他5 | | 【可用性】  サービス利用ができなくなるリスク（利用者が利用したいときに、提供できないことを含む） | 外部アクセス含め、アクセスコントロールが、有効に働かない | 他1 | | システム開発、保守、運用の管理の適切性が欠けている | 他2 | | 災害、破壊行為により、設備・機器等のリソースが使用不能となる | 他3 | | 開発要員、保守要員、運用要員のオペレーションミス防止策が有効でない | 他4 | | ウイルス等不正プログラム対策が不備である | 他5 | | |

**(記入例)【様式CS―3】**

|  |  |  |  |
| --- | --- | --- | --- |
| 20yy年mm月dd日  **CS言明書**  （会社名　　　　　　　　　　）  （役職　　　　　　　　　　　）  （氏名（自署）　　　　　　　）  当社は、下記クラウドコンピューティングサービスを提供するにあたり、「クラウド情報セキュリティ基本言明要件」（「クラウド情報セキュリティ管理基準」）の求めるところに従い、情報セキュリティガバナンスのもとで情報セキュリティマネジメントを実施し、基本リスクに対する管理策を整備、実装、運用しています。  1.クラウドコンピューティングサービス名称   |  | | --- | |  |   2.対象範囲   |  | | --- | | ○○○クラウドマネージドサービス　SaaS/PaaS/IaaS/DaaS/BaaS  ・IaaSサービス／PaaSサービス／DaaSサービスの場合  →サーバーリソースを提供するサービスにおいて当社の責任範囲は構内ネットワーク・ハードウェア・仮想化環境および初期提供状態のOSまでのインフラレイヤーとして定義します。  ※仮想マシン利用開始後のOSのパッチ等の更新、個別の仮想マシンのウイルス対策等については利用者側に更新責任が生じます    ・PaaSサービス／BaaSサービスの場合  →当社の責任範囲はサーバーネットワークなどのインフラおよび[提供するサービス機能]までを範疇とします。  当該機能を利用して構築された個別アプリケーションの動作により生じる範囲は各利用者側に管理責任が生じます。    ・SaaSサービスの場合  →当社の責任範囲はインフラ／ミドルウェア／アプリケーションが提供する機能までを範疇とします。  利用者アカウント管理やデータのサービス外へのバックアップ等は各利用者側の責任となります。  ・Security as a Service／API（API提供のみのサービス等）の場合  →当社の責任範囲は[提供するサービス機能]を範疇とします。[確実に提供者側責任となる分界点を明確化する]  　XXは各利用者側の責任となります。[不明瞭な分界点を明確化する]  なお、詳細については別途XXXを参照ください。 |   3.対象リスク   |  | | --- | |  | |

※1　申請時にCSマークの添付は不要です。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4.詳細言明   |  | | --- | | (1)情報の漏えいリスクに関して  当サービスでは、当社の管理下にあるクラウドコンピューティング内にあるお客さまの情報への、第三者の許可されないアクセスの防止について適切な管理策を施し、情報の漏えいリスクに対する管理策を行っています。  　※付1.対象リスク(詳細)に記載される(1)に対する対策を行っている場合  (2)情報と処理の改ざんリスクに関して  当サービスでは、クラウドコンピューティング内の情報及び処理が網羅されない、正確でない（改ざんされる等）によるリスクに対する管理策を行っています。  　※付1.対象リスク(詳細)に記載される(2)に対する対策を行っている場合  (3)サービス利用不能リスクに関して  当サービスでは、クラウドコンピューティングの特徴に起因するサービス停止や情報の利用阻害のリスクに対する管理策を行っています。  　※付1.対象リスク(詳細)に記載される(3)に対する対策を行っている場合  (4)その他の情報セキュリティリスクに関して  ISO/IEC27001及び27002に準拠した管理策を行っており、当社の内部監査フレームワークにより、その有効性を監査しています。  　※付1.対象リスク(詳細)に記載される(4)に対する対策を行っている場合 |   5.特記事項   |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | ○○○クラウドコンピューティングサービスの特性により、以下のリスクに関しては管理対象に該当いたしません。   |  |  |  | | --- | --- | --- | | セキュリティ要件／ リスクカテゴリー | リスク要因 | | | 機密性  保護すべき情報が漏えいするリスク | 国内外の法令等の開示、提出命令により、他利用者含め情報が開示され、またサービスが停止する | L19 | | 完全性  情報及び処理が改竄されるリスク |  |  | | 可用性  サービス利用ができなくなるリスク | 外部との相互運用性がなく、利用者のデータ移管、移行ができない（ロックイン） | L12 |   ・リスクの変化について  例：2015年７月より、IaaS基盤として既存のX社の×××サービスに加え、Y社の△△△サービスを利用開始しています。△△△サービスは×××サービスと同様のリスク管理を実施していることを確認しております。  例：2015年１月より、当社は■■■株式会社より当サービスの営業譲渡を受けました。  ・サービス利用者と当社間のＳＬＡ等の合意またはサービス契約に基づく個別事項に係るリスクについて、言明しておりません。  ・諸環境（内外の規制、技術等）の不可抗力の変化が、将来的に当社に及ぼすかもしれないリスクについて、言明しておりません。 | |