令和　　年　　月　　日

**協定締結希望申出書**

　神奈川県知事　黒岩　祐治　殿

住　　　　所

商号又は名称

代表者職氏名

神奈川県が募集する「県内事業者におけるＣＯ２排出量見える化促進に向けた連携協定」を締結したいので、関係書類を添付して提出します。

なお、次の誓約事項について誓約するとともに、暴力団又は暴力団員でないことを確認するため、役員等名簿（様式２）に記載した情報を神奈川県警察本部に照会することについて異議ありません。

【誓約事項】次の事項について相違ないことを誓約します。

1. 過去２年以内に銀行取引停止処分を受けていないこと。
2. 過去６か月以内に不渡手形又は不渡小切手を出していないこと。
3. 次の申立てがなされていないこと。
4. 破産法（平成16年法律第75号）第18条又は第19条の規定による破産手続開始の申立て
5. 会社更生法（平成14年法律第154号）第17条の規定による更生手続開始の申立て
6. 民事再生法（平成11年法律第225号）第21条の規定による再生手続開始の申立て
7. 債務不履行により、所有する資産に対し、仮差押命令、差押命令、保全差押又は競売開始決定がなされていないこと。
8. 安定的かつ健全な財政能力を有すること（債務超過の状況にないこと。）。
9. 県税その他の租税を滞納していないこと。
10. 神奈川県が措置する指名停止期間中の者でないこと。
11. 地方自治法施行令（昭和22年政令第16号）第167条の４の規定に該当する者でないこと。

（担当者連絡先）

　所在地　　　　：

　所属　　　　　：

　役職名・氏名　：

　電話番号　　　：

　メールアドレス：

**役員等名簿**

|  |  |
| --- | --- |
| 主たる事業所の所在地 |  |
| 商号又は名称のフリガナ（法人の組織商号は省略） |  |
| 商号又は名称（法人の場合は組織商号を含めて記載） |  |
| 代表者役職名 |  |
| 代表者氏名 |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 役職 | 氏名のフリガナ | 氏名 | 生年月日 | 性別 | 役員の住所 |
| 元号 | 年 | 月 | 日 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**同意書**

役員等名簿に記載された全ての者は、暴力団、暴力団員等、暴力団経営支配法人等に該当しないことを確認するため、当該役員等名簿を神奈川県に提出すること、及び神奈川県が当該役員等名簿に記載された情報を神奈川県警察本部に照会することについて、同意しております。

神奈川県知事 殿

令和　年　月　日

所　在　地

法　人　名

代表者（職・氏名）

情報セキュリティチェックリスト

| No | 確認事項 | 回答欄※回答にあたっては、「□」をチェック（「■」に変更）する。理由・意図等の補足が必要な場合は、備考に記述する。 |
| --- | --- | --- |
| 1 | ＣＯ２排出量管理システム提供事業者の情報セキュリティ関係に関する信頼性が十分であることを総合的・客観的に確認するため、各種の認定・認証制度の適用状況等を回答してください。（いずれかの認定・認証制度を取得している又は同等の取扱いを行っていることを、協定締結の要件の一つとします。） | 　□ISMAP　□ISO/IEC27017:2015　□ISO/IEC27018:2019　□ISO/IEC27001:2013又はISO/IEC27001:2022　□ISMAP-LIU（ISMAP for Low-Impact Use）　□クラウド情報セキュリティ監査制度（CSマークゴールド）　□クラウドサービス情報開示認定制度（ASPIC）　□その他（　　　　　　　　　　　　　　　　）備考： |
| 2 | 次の脆弱性等への対応が行われているか回答してください。(1) リリース前及び定期的に脆弱性診断（Webアプリケーション診断、プラットフォーム診断等）により脆弱性が含まれないことを確認すること。なお、脆弱性が発見された場合は対処が行われること。(2) 脆弱性に関する情報（OS、その他ソフトウェアのパッチ情報等）を定期的に収集し、パッチによる更新等の対処を実施すること。特に緊急を要する脆弱性については速やかにパッチによる更新等を行うこと。(3) サーバ、端末等にコンピュータウイルス等の不正プログラム対策ソフトウエアの導入等のセキュリティ対策を実施すること。また、不正プログラム対策ソフトウエアのパターンファイル等を常に最新に保つこと。 | (1)□適合　/　□不適合(2)□適合　/　□不適合(3)□適合　/　□不適合備考： |
| 3 | ＣＯ２排出量管理システム利用者の情報が保存されるサーバ等の設置場所（データの保管場所）が国内か国外かを回答してください。国外の場合、適用される国外法を記入してください。 | 　□国内　□国外　　適用される国外法：（　　　　　　　　　　） |
| 4 | 情報セキュリティインシデント対応に係る次の条件を満たしているか回答してください。* 1. 外部サービスを構成するシステムの稼働状況、障害、セキュリティインシデントを常時監視し、異常を検知できる仕組みがあること。
	2. 検知後、速やかに電話やメール等で通知を受けられる仕組みがあること。
	3. CSIRT（Computer Security Incident Response Team）又はセキュリティインシデント対応を行う体制があり、対処手順も整備されていること。
 | (1)□適合　/　□不適合(2)□適合　/　□不適合(3)□適合　/　□不適合備考： |
| 5 | 取り扱う情報の機密性保護のための通信及びストレージ・データに対する暗号化対策を講じているか回答してください。なお、暗号化は「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」において推奨された暗号技術等、安全性の高い技術を利用することとします。 | 　□適合　□一部適合（□通信　□ストレージ　□データ）　□不適合　理由（　　　　　　　　　　　　　　　　）備考： |
| 6 | 取り扱う情報の暗号化に用いる鍵の管理主体、管理手順等を明確にしているか回答してください。 | 　□適合　□不適合備考： |
| 7 | 悪意ある第三者等からの不正侵入、不正操作等の監視及び分析をするために必要なアクセス記録、システム稼動記録等のログを取得し、利用者が閲覧又は利用者に提供可能ですか。また、アクセス記録等のログの改ざん、窃取又は不正な消去の防止のために必要な措置を講じていますか。併せて、ログの保存期間は**１**年以上ですか。 | 　□利用者が閲覧又は利用者に提供可能なログ及び機能がある　　・閲覧・提供可能なログ（　　　　　　　　　　　）　　・保存期間　（　　年）　　・閲覧・検索等の機能　（□あり　□なし）　　・アクセス記録等の措置（□あり　□なし）　□閲覧・提供可能なログはない備考： |