デジサート PKI Class2 電子証明書利用規約

このデジサート PKI Class2 電子証明書利用規約（以下「**本 PKI Class2 証明書利用規約**」という）は、「クライアント証明書」（第 9 条に定義する）米国ユタ州法人 DigiCert, Inc.又は自己の関係会社（以下、総称して「**デジサート**」という）により、発行済み証明書で特定される個人（以下「**お客様**」という）に対し発行される PKI Class2 電子証明書（以下「**証明書**」(Certificate) という）に適用します。

その一部を構成するものとして「本 PKI Class2 証明書利用規約」を援用するマスターサービス契約書又はサブスクライバー契約書（当該契約書については、これらの条件（「ポータル」、「ポータルアカウント」、「ポータル API」、「QTPS サービス」、「適格証明書」、「QTPS」、「認証局適格トラストサービスプロバイダ」及び/又は評価用ライセンスに関連する条項を除く）と併せ、以下、総称して「**適用契約**」という）を承諾するか又は署名することにより、「お客様」は、以下を表明し、これを保証します：（i）（x）「お客様」のウェブサイトの真正性、及び（y）「お客様」が「証明書」のすべての利用に責任を有すること；及び（ii）「お客様」が発行される「証明書」に記載されるドメイン名を利用する独占的な権利を有すること。

「お客様」と「デジサート」は、以下のとおり合意します：

1. ユーザ

「お客様」は、「証明書要求者」(Certificate Requester)、「証明書承認者」(Certificate Approver)、そして「契約署名者」(Contract Signer)（「EV ガイドライン」に定義する）として行動し、「証明書」と「鍵ペア」の管理に関して「デジサート」と連絡を取り合うものとします。「**EV ガイドライン**」とは、CA/Browser Forum （以下「**CAB フォーラム**」という） が発行し、www.cabforum.org で公表される EV ガイドライン (Extended Validation Guidelines) を意味します。「お客様」は、以下を確約するものとします：（i）「お客様」は「デジサート」のサービスに関連するデータを「デジサート」が精査し、まとめ、収集し、そして「証明書」の更新とアップグレードを自動化する権限を付与します；（ii）「お客様」は、「お客様」が所有するか支配するドメイン名、IP アドレス又は資産の精査を自動化するためにのみサービスを利用するものとします；（iii）「お客様」は、「デジサート」により説明し販売されている目的で、「お客様」の意図したものについてのみ、https://www.digicert.com/legal-repository にあるデジサート利用規約 (DigiCert Acceptable Use Policy) に従ってサービスを利用するものとします。

2. 要求

「お客様」が「証明書」を要求できるのは、「お客様」について登録されたドメイン名に限定されます。「デジサート」は、その独自の裁量で「お客様」が単一の「証明書」に記載できるドメイン名の数を制限することができます。

3. 認証

「お客様」から「証明書」の要求を受領すると、「デジサート」はその要求を審査し、デジザート認証局運用規程並びに「証明書」発行に関連する適用法令を含む業界基準、ガイドライン及び要求事項（以下「**業界基準**」(Industry Standards) という）に従って、関連情報の認証を試みます。当該要求の認証は、「デジサート」の単独の裁量によるもので、「デジサート」は理由の有無を問わず、「証明書」の発行を拒否することができます。「証明書」発行要求を拒否した場合、デジザートは「お客様」に通知しますが、その理由を提示する義務はありません。「**認証局運用規程**」又は「**CPS**」とは、公開鍵インフラ（以下「**PKI**」という）を運営するために、「デジサート」が遵守する規約と業務を文書化したものを意味し、適用されるタイムスタンプ方針及び表明 (Time-Stamp Policies and Statements) を含みます。「デジサート」の「CPS」は、https://www.digicert.com/legal-repository で入手することができます。「QTSP」（「QTSP」としての資格において行為するかどうかにかかわらず）又は関係会社から発行されたサービス用「CPS」は、https://www.quovadisglobal.com/repository で入手することができます。

4. 証明書のライフサイクル

発行された「証明書」のライフサイクルは、「証明書」申請時の「お客様」の選択、「CPS」の要件事項、及び「証明書」の意図された用途によります。「デジサート」は、以下の要件事項を遵守するために、必要に応じて未発行の「証明書」の「証明書」ライフサイクルを変更することができます：（i）「適用契約」；（ii）「業界基準」；（iii）「デジサート」の監査人；又は（iv）「アプリケーション・ソフトウェアベンダー」。「**アプリケーション・ソフトウェアベンダー**」(Application Software Vendor) とは、「デジサート」が加盟しているか、加盟する配布されたルートストア（root store）に関連して、「証明書」を表示するか使用する団体を意味します。「お客様」は、「証明書」の終了日後、又は「デジサート」が「適用契約」で許可されたとおり「証明書」を失効させた後は、「証明書」そしてそれに関連する「秘密鍵」（以下に定義する）の使用を停止することに同意し

ます。

5. 発行

「証明書」の認証が「デジサート」の満足する程度に完了した場合、「デジサート」は申請された「証明書」を発行し、合理的な方法によって「お客様」に交付します。一般的に、「デジサート」は、そのウエブサイトを介して「証明書」を電子的に納品します。「デジサート」は、「証明書」の発行に使用する「ルート証明書」や「中間証明書」を、「お客様」への通知なくいつでも変更することができます。「お客様」は、「証明書」の申請と利用にあたり、米国輸出管理及び経済制裁法令を含むすべての適用法令、規制、及び「業界基準」に従うものとします。「お客様」は、米国財務省外国資産管理局 (United States Treasury Department's Office of Foreign Assets Control)、米国商務省 (United States Commerce Department)、欧州委員会 (European Commission)、英国財務省金融制裁実施庁 (United Kingdom HM Treasury's Office of Financial Sanctions Implementation) 又は「デジサート」に管轄権を有するその他の関連政府機関によって制限されている国又は地域では「証明書」は利用できないことを確認します。

6. 証明書ライセンス

納品後直ちに有効となり、そして「証明書」が終了するか又は失効するまで継続的に、「お客様」は「証明書」の対象被認証者の利益のために、発行された各「証明書」と対応する「鍵ペア」を、全ての適用法令、規制、「業界基準」及び「本 PKI Class2 証明書利用規約」の条件に従って、「CPS」に記載された目的のために利用することができます。「**鍵ペア**」(Key Set) とは、（i）「公開鍵」はメッセージの暗号化を行い、そしてそれを復号化できるのは「秘密鍵」のみであり、そして（ii）「公開鍵」がわかっていても、「秘密鍵」を読み取ることは計算的に不可能とすることを特徴とする、2 つ又はそれ以上の数学的に関連する鍵を意味し、「秘密鍵」又は「公開鍵」に伴う鍵の共有と呼ばれます。「お客様」は、「証明書」又は「秘密鍵」の不正使用を発見した場合、直ちに「デジサート」に通知するものとします。「お客様」は、「証明書」の申請や使用、又はエンドユーザやシステムに頒布するために必要な認可やライセンス（米国輸出規制法令で要求されるライセンスを含む）を取得し、維持する責任を負うものとします。SSL「証明書」は、一度に一以上の物理サーバー又は端末上で使用することができます。但し「デジサート」は、追加サーバー又は端末上での「証明書」の使用について料金を請求することができるものとします。

7. 鍵ペア

「**秘密鍵**」(Private Key) とは、「お客様」が機密にしている鍵で、電子署名の作成、及び／又は対応する「公開鍵」で暗号化された電子記録やファイルを復号化するために使われる鍵を意味します。「**公開鍵**」(Public Key) とは、「お客様」が一般に公表している鍵で、「お客様」の「証明書」に記載され、「お客様」が使用している「秘密鍵」に対応するものを意味します。「お客様」は（i）信頼できるシステムを用いて「鍵ペア」を作成し、（ii）少なくとも RSA 2048 ビット鍵と同等の「鍵ペア」を使用し、及び（iii）すべての「秘密鍵」を機密に保持する必要があります。「秘密鍵」を保護しなかった場合、「お客様」は全責任を負うものとします。その他の種類の「証明書」については、安全なソフトウェアかハードウェア・システム上に保存することができます。「お客様」は、「適用契約」に従って「デジサート」により生成された「鍵ペア」を、その地域の適用法令、規則及び規制に従って取得、使用又は受領する責任があるものとします。適用法令、規則、及び規制には、「お客様」が対象の「鍵ペア」を取得、使用、又はその他受領する裁判管轄内の輸出入規制法、規則、及び規制が含まれますが、それらに限定されるものではありません。「お客様」が特定の「デジサート」のサービスに関して「秘密鍵」（その複製を含む）をインポート又はエクスポートすることを許可されている場合、「デジサート」は「お客様」に対し、適用されるサービスで作成されていないか、若しくは「秘密鍵」（その複製を含む）が適用されるサービスからエクスポートされた後を含め，当該サービス外で使用されている「お客様」の「秘密鍵」（その複製を含む）の使用又は保管について責任を負わないものとします。

8. 証明書の透明性

「証明書」がそのライフサイクルを通して適切に機能するように、「デジサート」は一般に公開されている証明書透明性データベースに「証明書」を記録することができます。ログサーバの情報は、一般に公開されています。いったん提出された情報は、ログサーバから削除することはできません。

9. クライアント証明書

「**クライアント証明書**」(Client Certificate) とは、コードサイニング署名 (codeSigning)、タイムスタンプ (timestamping)、又はサーバ認証 (serverAuthentication) 以外のすべての拡張鍵用途 (extendedKeyUsage) を含む「証明書」を意味します。「クライアント証明書」には多種多様な使用用途があり、そしてそれは「クライアント証明

書」のプロファイルで定義されています。「クライアント証明書」のプロファイルで定義される利用法として、電子署名や電子メールの暗号化、及び暗号認証などがあります。「お客様」が「クライアント証明書」を要請する場合は、「お客様」は：（i）「CPS」の規定に従い、適切な社内文書を使って、申請者の身元と所属を確認し、そして（ii）「クライアント証明書」中の提供された情報、及び「クライアント証明書」に関連するか、又はその一部を構成する表明が、すべての重要な点において真実、完全、そして正確であることを確認しなければなりません。

10. 管理

通常「デジサート」は、お客様」の指示に従い、「証明書」を発行、管理、更新し、及び失効させますが、これは当該指示の正確性に対する「デジサート」の信頼を基礎とします。「お客様」は、「デジサート」との通信にあたっては正確で完全な情報を提供するものとし、当該情報に何らかの変更があった場合、5「営業日」以内に「デジサート」に通知するものとします。「お客様」は、「お客様」が提供した情報の有効性について「デジサート」から質問があった場合、当該質問の通知を受領してから 5「営業日」以内に返答するものとします。「お客様」は、「証明書」を使用する前に「証明書」データが正確であるか照合し、そして確認するものとします。「証明書」は、発行から 30 日後、又はそれ以前であっても「お客様」が「証明書」を使用した証拠が存在する場合はその使用時に、承認されたものと見なされます。「デジサート」は、有効期限切れが迫った「証明書」に関する通知を送信することができますが、それを行う義務はなく、有効期限が切れる前に「証明書」を確実に更新する責任は、全面的に「お客様」にあるものとします。「**営業日**」とは、米国連邦規則集第 5 巻パート 6103 で規定されている米国の連邦祝日を除く月曜日から金曜日を意味します。

11. 鍵ペアのセキュリティと使用

「お客様」は、「証明書」と関連づけられている「鍵ペア」を安全に生成、保護し、そして「秘密鍵」の危殆化、紛失、不正使用を防ぐために必要なすべての手段を講じるものとします。「お客様」は、ベストプラクティスを満たすよう、「CAB フォーラム」で定めるネットセキュリティ要件及びその他の関連要件を満たすパスワードを使用するものとします。「お客様」は、その従業員、代理人や委託業者が「お客様」による（法律で許可される範囲の）身元調査と、「PKI」及びその他の情報セキュリティ分野の研修を受けているか、又は経験を有している場合にのみ、該当する従業員、代理人や委託業者にのみ、「秘密鍵」へのアクセス又は使用を許可するものとします。以下の場合、「お客様」は「デジサート」に通知をし、「証明書」とそれに紐づけられた「秘密鍵」の失効を要請し、当該「証明書」とそれに紐づけられた「秘密鍵」の使用を停止し、そして当該「証明書」がインストールされたすべてのデバイスから「証明書」を削除するものとします：（i）「証明書」のいずれかの情報が間違っているか正確でない又は正確でなくなる場合；又は（ii）「証明書」に含まれる「公開鍵」に紐づけられた「秘密鍵」の悪用又は危殆化が起こったか又は起こったことが疑われる場合。コードサイニング「証明書」に関しては、以下の状況であると「お客様」が判断した場合、速やかに「証明書」とそれに紐づく「証明書」の「秘密鍵」の使用を停止し、「証明書」の失効を要請するものとします：（a）「証明書」のいずれかの情報が間違っているか不正確である場合；（b）「証明書」に含まれる「公開鍵」に紐づけられた「秘密鍵」が悪用又は危殆化された場合；あるいは（c）「サスペクトコード」に署名するために「証明書」が使用された証拠がある場合。「**サスペクトコード**」(Suspect Code) とは、有害又は悪意のある機能、又は深刻な脆弱性を含むコード（スパイウェアやマルウェア、ユーザの承認なくインストールされ、及び／又は削除できないその他のコード、ならびにそれが実行されるプラットフォームの信頼性を失わせるような設計者の意図していない方法で利用可能なコードなどを含む）を意味します。お客様」は、異なる「証明書」の種類に同一の「秘密鍵」使用しないものとします。例えば、「お客様」は、コードサイニングに使用する「秘密鍵」を非コードサイニング「証明書」を要求するために使用しないものとします。「デジサート」が、ある特定の種類の「証明書」又はアクション（例えば、コードサイニング）に使用されている「秘密鍵」が異なる種類の「証明書」（例えば、TLS/SSL「証明書」又は「クライアント証明書」）を要求するために利用されていることを発見した場合、「デジサート」は、当該「秘密鍵」又はその他の「デジサート」により発行された関連する「鍵ペア」に関連付けられた全ての「証明書」を失効しなければならないものとします。「お客様」は、「鍵ペア」の危殆化や「証明書」の悪用に関する「デジサート」の指示に 24 時間以内に応答しなければならないものとします。「お客様」は、以下のいずれか早く到来する時に、「証明書」に対応する「鍵ペア」の使用を停止するものとします：（I）「証明書」が失効された時；及び（II）許可されている「鍵ペア」の使用期間が切れた時。「お客様」は「証明書」の失効後は使用を停止しなければならないものとします。

12. 証明書の欠陥

「証明書」の不備（以下「**不備**」という）に対する「お客様」の唯一の救済策は、「お客様」から該当「不備」の通知を受け取った後、当該「不備」を是正すべく商業的に合理的な努力をするよう「デジサート」に要請する

ことのみになります。以下の場合は、「デジサート」は「不備」を是正する義務はありません：（i）「お客様」による「証明書」の悪用や損壊、又は改造があった場合；（ii）「お客様」が「デジサート」に速やかに「不備」の報告をしなかった場合；又は（iii）「お客様」が「適用契約」のいずれかの条件に違反した場合。

13. 依拠当事者保証

「お客様」は、「依拠当事者保証」が依拠当事者の利益のためだけのものであることを確認します。「**依拠当事者保証**」(Relying Party Warranty) とは、「デジサート」のウェブサイト https://www.digicert.com/legal-repository に掲載される、依拠当事者契約 (Relying Party Agreement) と限定保証 (Limited Warranty) の条件を満たす、依拠当事者に提供される保証を意味します。「デジサート」の関係会社から発行された「証明書」に対する「依拠当事者保証」は、https://www.quovadisglobal.com/repository にあるウエブサイトに掲載します。「お客様」には、「依拠当事者保証」の条件を強制する権利、又は「依拠当事者保証」に基づく請求を行う権利を含め、「依拠当事者保証」に基づく一切の権利はありません。「**依拠当事者**」(Relying Party) とは、「依拠当事者保証」に規定される意味を持つものです。「アプリケーション・ソフトウェアベンダー」は、それが提供するソフトウェアが「証明書」に関する情報を表示するだけであったり、あるいは「証明書」や電子署名の使用を斡旋するだけであったりする場合は、「アプリケーション・ソフトウェアベンダー」は「依拠当事者」とはなりません。

14. 表明

申請される各「証明書」について、「お客様」は以下を表明し保証します：

a. 「お客様」は（i）「証明書」で指定されているすべてのドメイン名、及び（ii）「証明書」で指定されているすべてのコモンネーム又は団体名を使用する権利を有しているか、又は正当な所有者であること；
b. 「お客様」は、権限を与えられた、合法的な目的にのみ「証明書」を使用すること。これには、「サスペクトコード」を署名する為に「証明書」を使用しないこと；「証明書」と「秘密鍵」をすべての適用法令に準じ、「証明書」の目的、「CPS」、適用される証明書ポリシー、及び「適用契約」に従ってのみ使用すること。
c. 「お客様」は「CPS」を読み、理解し、そしてそれに同意すること。
d. 「CPS」又はパブリック証明書の発行及び管理に関する基本要件 (Baseline Requirements) の違反があった場合、「お客様」は速やかに「デジサート」に通知し、及び
e. 「証明書」に含まれる団体と登録されたドメイン名の所有者が、各「証明書」申請を認知し、承認すること。

15. 制限

「お客様」は以下を行わないものとします：

a. 「デジサート」のシステム又はソフトウェアの技術実装を監視、妨害又はリバースエンジニアリングしたり、又はその他「デジサート」のシステム又はソフトウェアのセキュリティを故意に危殆化すること；
b. 第三者の知的財産権を侵害する「証明書」情報を「デジサート」に提出すること；又は
c. 「デジサート」又は第三者の「秘密鍵」に実質的に類似した「秘密鍵」を故意に作成すること。

16. 証明書の失効

「デジサート」は「CPS」に記載される理由により、通知なく「証明書」を失効させることができますが、それには次のいずれかに該当すると「デジサート」が合理的に考える場合も含まれます：

a. 「お客様」が「証明書」の失効を申請したか、「証明書」の発行を許可しなかった場合；
b. 「お客様」が「適用契約」、又は「CPS」上の義務に違反した場合；
c. 「お客様」との契約の条項で、「証明書」の発行や使用、管理、又は失効に関連する表明又は義務を含むいずれかが解除されるか無効とされた場合；
d. 「お客様」が政府の取引禁止対象とされている個人又は団体リストに追加されるか、又は米国の法律で輸出禁止対象とされている仕向地から事業を行なっている場合；
e. 不正確又は誤解を招くような情報が「証明書」に含まれている場合；
f. 「証明書」が、意図された目的以外に許可なく使用された場合又は「サスペクトコード」に署名するために

使用された場合；

g. 「証明書」に関連付けられた「秘密鍵」が開示又は危殆化された場合；

h. 「証明書」が（i）悪用された場合；（ii）法律や「CPS」又は「業界基準」に反して使用されるか発行された場合；又は（iii）フィッシング攻撃、詐欺、マルウェアの配信、その他の違法若しくは詐欺行為目的、又はデジサート利用規約 (DigiCert Acceptable Use Policy) に概説されるその他の違反行為などの違法若しくは詐欺行為目的で直接的又は間接的に使用された場合；又は

i. 「業界基準」又は「デジサート」の「CPS」により、「証明書」の失効が必要とされる場合、又は「デジサート」や第三者の権利、機密情報、事業、又は評判を保護するために失効が必要な場合。

17. 情報の共有

以下の場合、「デジサート」は、「お客様」、「証明書」で署名されたアプリケーション又はオブジェクト、「証明書」、そして周辺環境に関する情報を、他の認証局や「CAB フォーラム」を含む業界団体と共有する権限を有していることを、「お客様」は承認し、そして受諾するものとします：（i）「証明書」又は「お客様」が「サスペクトコード」のソースであると同定された場合；（ii）「証明書」を申請するための権限が認証できない場合；又は（iii）「お客様」の申請以外の理由で「証明書」が失効された場合（たとえば「秘密鍵」の危殆化、マルウェアの発見などの結果）。

18. 業界基準

両当事者は、「証明書」に適用されるすべての「業界基準」と法律を遵守するものとします。適用法令や「業界基準」が変更され、その変更が「証明書」又は「適用契約」により提供されるサービスに影響する場合、「デジサート」は、その変更を遵守するために必要な限度で、サービスを変更若しくは「適用契約」を改正、又は終了させることができます。

19. 設備

「お客様」は、自らの費用で以下について責任を有するものとします：（i）「証明書」と関連する「デジサート」のソフトウェア又はサービスを利用するのに必要な、すべてのコンピュータ、通信機器、ソフトウェア、インターネット接続、そして通信ネットワーク（それが必要な場合）；及び（ii）「お客様」の業務ならびに「お客様」のウェブサイトの保守、運営、開発そしてコンテンツ。

20. 証明書の受益者

「依拠当事者」と「アプリケーションソフトウェアベンダー」は、「証明書」の使用と発行に関する「お客様」の義務と表明の明示的な第三受益者です。「依拠当事者」と「アプリケーションソフトウェアベンダー」は、いかなる「デジサート」のソフトウェアに関しても、その明示的な第三受益者ではありません。

21. エンドユーザライセンス契約（EULA）と第三者の条件

a. 装置又はデバイスへのインストール用ソフトウェア（以下「**許諾ソフトウェア**」という）としての「お客様」による「デジサート」サービス（又はそのコンポーネント）の利用は、「許諾ソフトウェア」に付属するライセンス契約に準拠するものとします。ただし、「許諾ソフトウェア」にライセンス契約が付属しない場合は、当該「許諾ソフトウェア」の使用は、http://www.digicert.com/eula にあるソフトウェア・エンドユーザー・ライセンス契約（「以下 **EULA**」という）に準拠するものとします。

b. 「お客様」は、「お客様」の「証明書」に Ubisecure 社により提供される取引主体識別子 (legal entity identifier)（以下「**LEI**」という）が含まれる場合、https://rapidlei.com/documents/global-lei-system-terms/ から入手可能な RapidLEI サービス利用規約 (RapidLEI Terms of Service) が、「お客様」の LEI と、RapidLEI 取引主体識別子管理システム又はその後継サービスの使用に適用されることを認識し、同意するものとします。

c. 「お客様」による「デジサート」の耐量子暗号ツールキット (post-quantum cryptographic toolkit)（以下「**PQC ツールキット**」という）の使用は、次の条件に従うものとします：（i）「お客様」に対して許諾される「PQC ツールキット」に関するライセンスは非独占的で、解除可能なライセンスであり、当該ライセンスは「PQC ツールキット」又は関連検査と設定活動により生成された署名と「公開鍵」を含む「デジサート」の「証明書」についてのみ使用します；（ii）「お客様」は、「PQC ツールキット」又はそれに関連する知的財産に係る知的財産権又はその他の専有権を一切取得するものではありません；（iii）「お客様」は、「PQC ツールキット」に対して、リバースエンジニアリング、翻訳、逆アセンブル、逆コンパイル、復号、又は破

壊を行いません；（iv）「お客様」は、「デジサート」の関連サービス終了時に「PQC ツールキット」の使用を中止します；（v）ISARA 社は、いかなる損害についても「お客様」に対して責任を負いません；（vi）「お客様」は、「PQC ツールキット」が使用又は輸入された国又は地域、若しくは「PQC ツールキット」が輸出又は再輸出された国又は地域の適用法令に従ってのみ「PQC ツールキット」を輸入、輸出及び再使用するものとします；（vii）「デジサート」は ISARA 社に代わって明示黙示の如何を問わず「PQC ツールキット」に関連する保証を一切行いません；及び（viii）「お客様」は「PQC ツールキット」又は関連資料に含まれる著作権、商標又は特許表示を変更しないものとします。

d. 「お客様」が「デジサート」から Thales, Gemalto 又は SafeNet 製品又はサービスを購入する場合、当該製品又はサービスの「お客様」による使用は、https://cpl.thalesgroup.com/legal で入手可能な Thales エンドユーザーライセンス契約書 (Thales End User License Agreement) に従うものとし、「デジサート」を介した Thales のクラウドベースサービスの購入は、https://www6.thalesgroup.com/service-specific-terms で入手可能な条件に従うものとします。

22. フローダウン要件

「お客様」は、「デジサート」のシステム又はソフトウェアのセキュリティの技術的実装を監視、妨害、リバースエンジニアリングしたり、又はその他の方法で危殆化しないものとし、また指定された製造業者がある場合、同様の義務を課すものとします。

23. 通知

「適用契約」の別段の定めにかかわらず、「本 PKI Class2 証明書利用規約」により容認されるか又は要求されるすべての通知は電子メール（以下「**E メール**」という）によるものとし、全国的に有名で信用のある SMPT 配信サービスによる送信と同時に交付及び受領されたものとみなします。通知は記録された宛先に配信するものとし、「デジサート」に対する場合 class2_support_jp@digicert.com に、「お客様」に対する場合 「お客様」が随時指定する「E メール」アドレスに配信するものとします。

[以下余白]