Confidential

クラウド 帳票発行サービス
SPF・DKIM・DMARC の設定

更新日：2024/03/12

MUFG 三菱UFJ銀行

1.SPF レコードとは

SPF レコードとは、送信元ドメインが他のドメインになりすましされていると受信元サーバ（お客様側）で判断されてしまうことを防ぐ仕組みです。

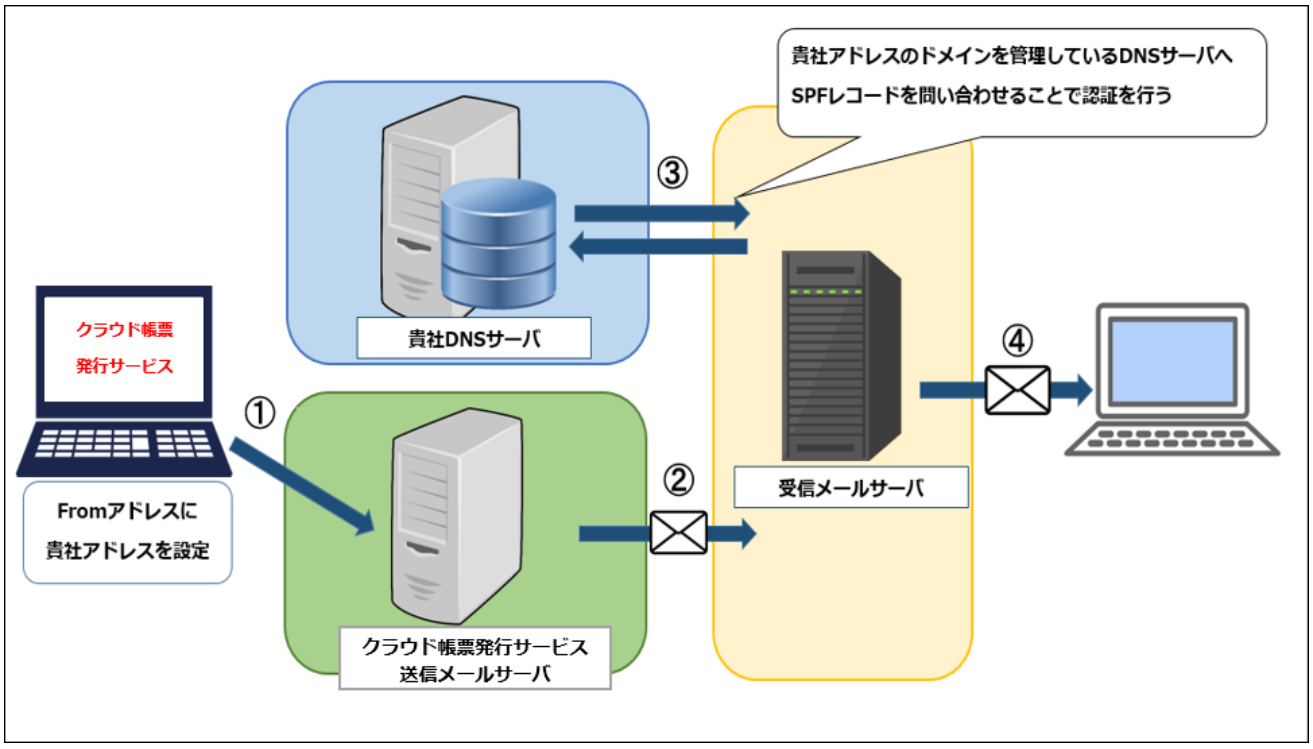
SPF レコードを設定すると？

クラウド帳票発行サービスからのメール受信時に、お客様側の受信メールサーバは、送信元アドレス（貴社アドレス）を管理している DNS サーバへ SPF レコードを問い合わせます。

※DNS サーバとは：「ドメイン名」を管理しているサーバです。

貴社 SPF レコード内でクラウド帳票発行サービスサーバが許可されていない場合は、 ドメインのなりすましが行われたと判断して受信を拒否されてしまう可能性がございます。

次項でご案内する SPF レコードを、貴社 DNS サーバに追記することで、クラウド帳票発行サービスから送信されるメールが迷惑メールとして判断されにくくなります。



2.SPF レコードの設定

クラウド帳票発行サービスから送信されるメールが迷惑メールと判断されないよう、下記手順を参考に貴社DNS サーバへ SPF レコードの設定をお願いいたします。

■注意

SPF レコードの記載については、お客様ごとに内容が異なる可能性が高いため、弊社からは一般的な記載方法のご案内のみとなります。
詳細な設定方法については、貴社のサーバ管理者様（またはサーバ管理会社）にご確認くださいますようお願いいたします。

■設定手順

【１】「お客様向けメールの From アドレス」を確認する

管理画面　＞　基本設定　＞　通知メール設定画面　＞

「お客様向けメールの From アドレス」に設定されているメールアドレスを確認します。

こちらのメールアドレスを運用（設定）しているサーバ管理者様（またはサーバ管理会社）を確認します。

【２】サーバ管理者様へ設定方法の確認

【1】で確認したサーバ管理者様（またはサーバ管理会社）に以下の内容のご確認（または設定依頼）をお願いいたします。

＜確認内容＞

①.【１】で確認したメールアドレスに対して、SPF（TXT）レコードの設定はできるのか？

②.設定出来る場合、具体的な設定方法は？

③.【１】で確認したメールアドレスを運用（設定）しているメールサーバのグローバル IP アドレスは何か？

※メールサーバのグローバル IP アドレスがわからない または 教えられないといった場合、
「公開済み SPF レコードは存在するでしょうか？また該当の SPF レコードを教えていただけないでしょうか？」とお尋ねください。

【3】サーバへ SPF レコードを登録

【2】で SPF（TXT）レコードの設定ができることを確認した場合、またはサーバ管理者様（またはサーバ管理会社）から提示された設定方法に従って、SPF レコードの設定を行います。
ここでは TXT レコードへ include を利用し追記する方法をご案内いたします。

▼include を利用して設定する場合の記述例

---

rakus.co.jp. IN TXT "v=spf1 ip4: <メールサーバ IP> include:chohyo-bpo★.bk.mufg.jp ~all"

・上記ドメインの★部分は、お客様に提供させて頂く本番環境によって異なります。実際に提供させて頂くドメインに応じて、上記 include 以降の★部分の変更をお願いいたします。

※★部分の値については、サポートセンターまでお問い合わせください。
また、★部分の確認は本番環境提供時に可能となるため、本設定は本番環境提供後に実施をお願いいたします。

・上記「rakus.co.jp」は貴社ドメイン名への変更をお願いいたします。
・上記「メールサーバ IP」は【２】で確認したメールサーバのグローバル IP アドレスに置き換えます。

※既に SPF レコードが存在する場合は、上記のうち「include:chohyo-bpo★.bk.mufg.jp」のみを既存の SPF レコードに追加してください。
※【２】でメールサーバのグローバル IP アドレスが判明せず、SPF レコードを聞いた場合、以下のような記述で SPF レコードを設定してください。

---

rakus.co.jp. IN TXT "v=spf1 include: <公開済み SPF レコード> include:chohyo-bpo★.bk.mufg.jp ~all"

3.SPF レコードの設定確認方法

SPF レコードが正しく設定されているか確認する方法の一例として、外部サイトを利用した確認方法をご案内いたします。（※外部サイトの動作保証は致しかねますので、ご了承ください。）

SPF レコードの設定から結果反映まで時間がかかるケースがございます。
設定作業実施日から 1 日程度、時間を空けてご確認をお願いいたします。

SPF Surveyor – dmarcian（外部サイト）

https://dmarcian.com/spf-survey/

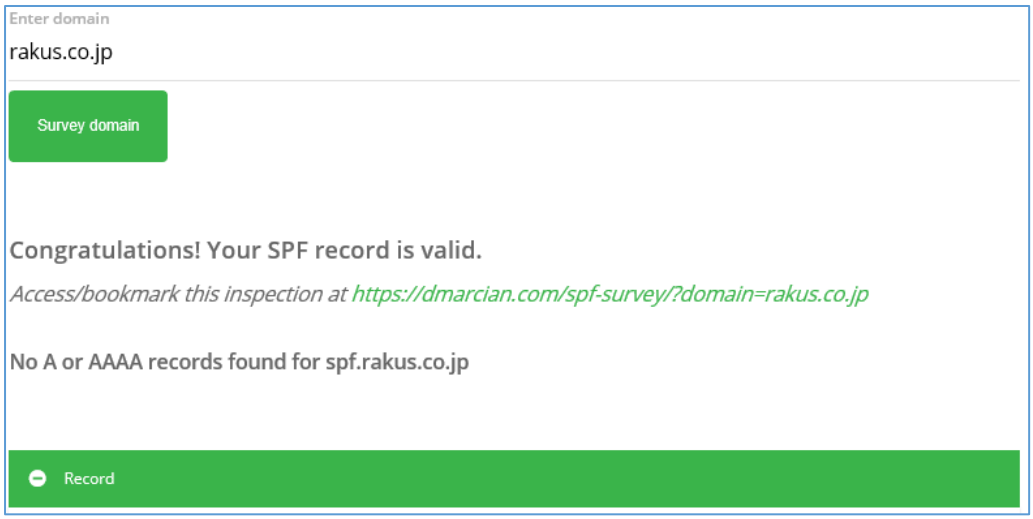
▼利用方法

①「Enter domain」エリアに貴社メールアドレスのドメインを入力
※「XXX@●●.co.jp」の場合、●●.co.jp を入力
※@は含めない

②「Survey domain」をクリック

③チェック結果が表示されます。
画面に“Your SPF record is valid.”という記述があり、「Record」がグリーンで表示されていれば、SPF レコードが有効となっています。
また、有効になっていても「Record」に表示されている TXT レコード内に、「2.SPF レコードの設定」で設定した TXT レコードが存在しない場合、クラウド帳票発行サービスのサーバが正しく記述されておりません。

成功時（例）：



エラー判定となってしまった場合は、今一度、サーバ管理者様（またはサーバ管理会社）へお問い合わせください。※外部サイトのため画面イメージが変更になる場合がございます。予めご了承くださいませ。

4.DKIM の設定

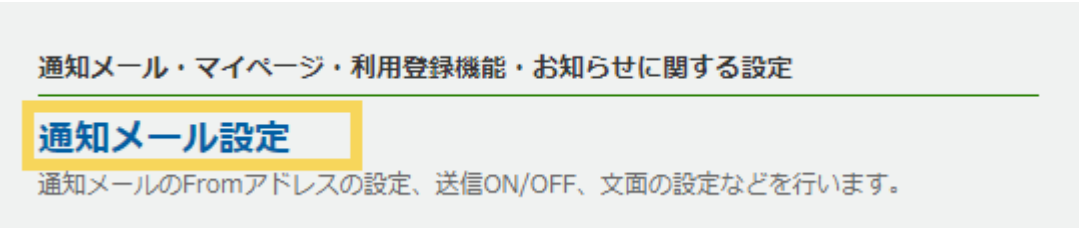
■DKIM とは

DKIM とは、メールの受信側サーバで送信元ドメインのなりすましやメール改ざんの疑いがあると判断されてしまうことを防ぐ仕組みです。DKIM を設定しない場合、クラウド帳票発行サービスから送信したメールが迷惑メールとして振り分けられたり、受信を拒否されてしまう可能性があります。
DKIM の設定を行うことで、クラウド帳票発行サービスから送信されるメールが迷惑メールとして判断されにくくなります。

■設定手順

※作成者署名で DKIM 設定を行う場合は、事前に貴社メールアドレスのドメインを管理する DNS サーバに公開鍵を設定する必要があります。設定方法については、貴社 DNS サーバの管理者様（またはサーバ管理会社）にご確認ください。
公開鍵の作成方法は、「秘密鍵と公開鍵の作成手順」ページをご確認ください。

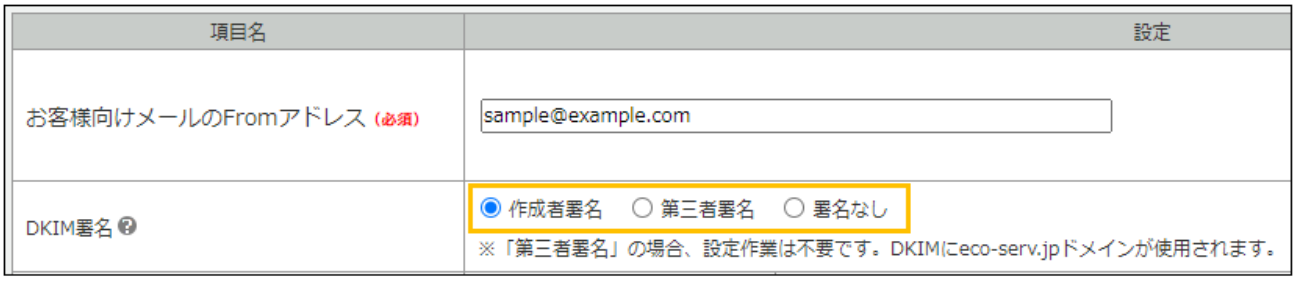
①管理画面　＞　基本設定　＞　通知メール設定　画面に遷移します。



②「編集」をクリックします。

	項目名	設定
編集	お客様向けメールのFromアドレス	sample@example.com
	スタッフ向けメールのFromアドレス	sample@example.com
	お客様向けメールの署名	設定されていません。

③DKIM の署名方法を選択します。



作成者署名（推奨）	送信するメールがなりすましメールと判断されないよう、原則こちらを利用してください。「作成者署名」を利用する場合は、手順④に沿って DKIM 設定を行ってください。
第三者署名	「作成者署名」に必要な DKIM 設定を行うことができない場合に選択してください。DKIM に eco-serv.jp ドメインが使用されるため貴社での DKIM 設定は不要ですが、作成者署名よりも送信するメールがなりすましメールとして判断される可能性が高くなります。
署名なし	「作成者署名」を設定できず、「第三者署名」を設定したくない場合のみ選択してください。DKIM 署名を行わないため、第三者署名よりも送信するメールがなりすましメールとして判断される可能性が高くなります。

④③で「作成者署名」を選択した場合は、DKIM 設定に必要な内容を入力します。

セレクタ	任意の名称を入力してください。 ※セレクタとは、公開鍵・秘密鍵の名称となる任意の名前です。
ドメイン	貴社メールアドレスのドメインを入力してください。
秘密鍵	貴社で作成した秘密鍵の情報を入力してください。 秘密鍵の作成方法は「秘密鍵と公開鍵の作成手順」ページをご確認ください。
公開鍵	貴社メールアドレスのドメインを管理する DNS サーバに、公開鍵の内容を設定してください。設定方法については、貴社 DNS サーバの管理者様（またはサーバ管理会社）にご確認ください。公開鍵の作成方法は「秘密鍵と公開鍵の作成手順」ページをご確認ください。 ※DNS サーバの設定が済んでいない場合、設定変更時にエラーが発生します。

秘密鍵・公開鍵は RSA 形式で用意してください。

5.秘密鍵と公開鍵の作成手順

DKIM 設定を行う場合、貴社にて秘密鍵と公開鍵をご用意いただく必要があります。

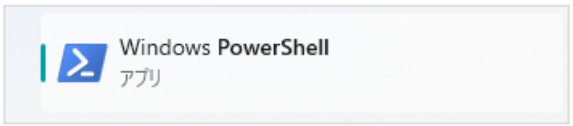
下記手順を参考に、秘密鍵と公開鍵の作成をお願いいたします。

※本マニュアルでは、作成手順の一例を記載しております。
※作成手順は windows11 のご利用を前提に記載しています。ご利用の OS によっては手順が異なる場合があります。
※秘密鍵・公開鍵は RSA 形式でご用意いただく必要があります。

▼作成手順

①Windows の検索ボックスに「Powershell」と入力します。

「Windows Powershell」のアプリが検索結果に表示されるので、クリックして起動します。

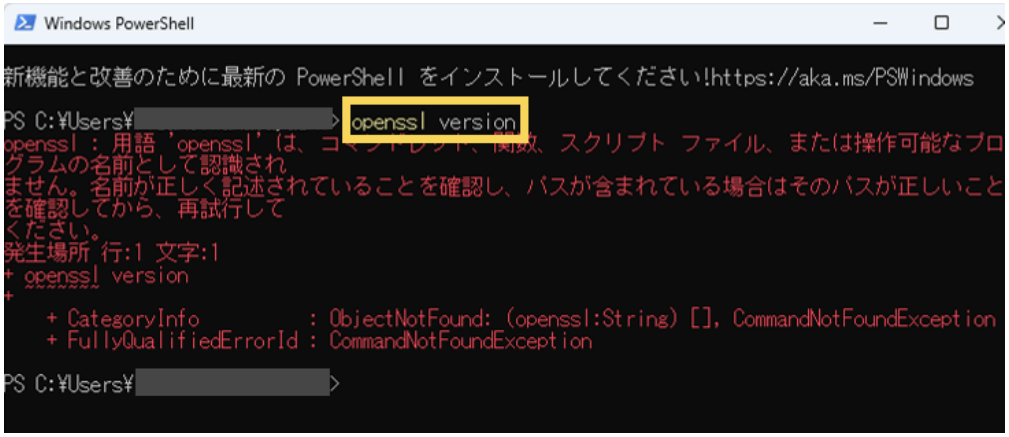


②「OpenSSL」がインストールされているか確認します。

「openssl version」を入力し、エンターキーを押します。以下の通りエラーが発生したら、

「OpenSSL」

はインストールされていませんので一度「Windows Powershell」を閉じて手順③に進みます。



以下の通り「OpenSSL 1.1.1w 11 Sep 2023」といったバージョン情報が表示された場合は、既に

「OpenSSL」がインストールされているので手順⑳に進みます。

③「OpenSSL」をインストールします。以下 URL にアクセスします。（外部サイトに遷移します）

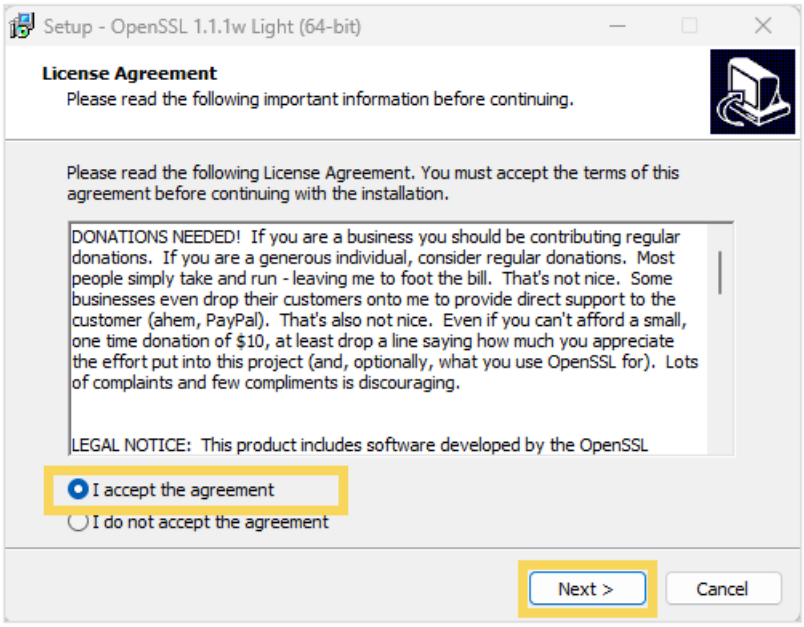
https://slproweb.com/products/Win32OpenSSL.html

④「Win64 OpenSSL v1.1.1w Light」の「EXE」をクリックしてファイルをダウンロードします。

Win64 OpenSSL v1.1.1w Light EXE | MSI	4MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.1w (Recommended for users by the creators of OpenSSL). this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of
Win64 OpenSSL v1.1.1w EXE | MSI	65MB Installer	Installs Win64 OpenSSL v1.1.1w (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit v OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1w Light EXE | MSI	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.1w (Only install this if you need 32-bit OpenSSL for Windo More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.1w EXE | MSI	55MB Installer	Installs Win32 OpenSSL v1.1.1w (Only install this if you need 32-bit OpenSSL for Windows). Note that this is a default build of legal agreement of the installation.

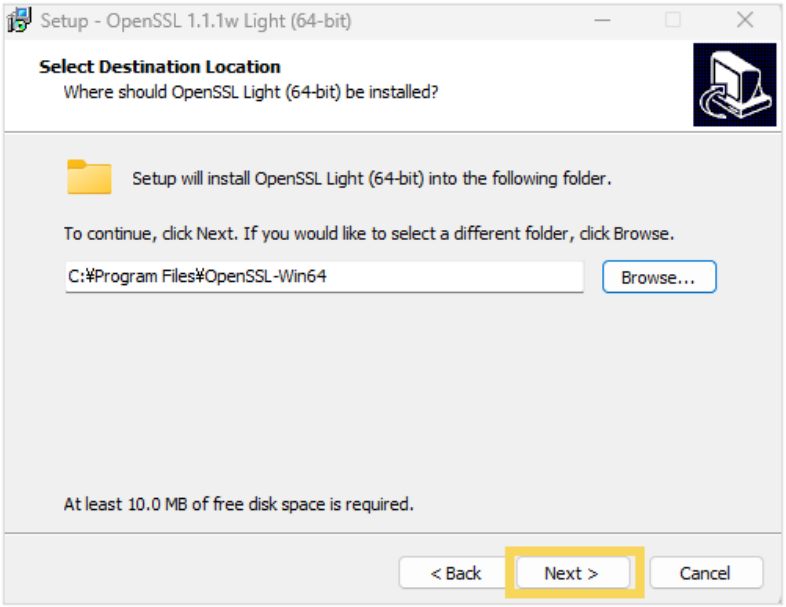
⑤ダウンロードしたファイルをダブルクリックして起動します。

⑥「I accept the agreement」を選択して「Next」をクリックします。

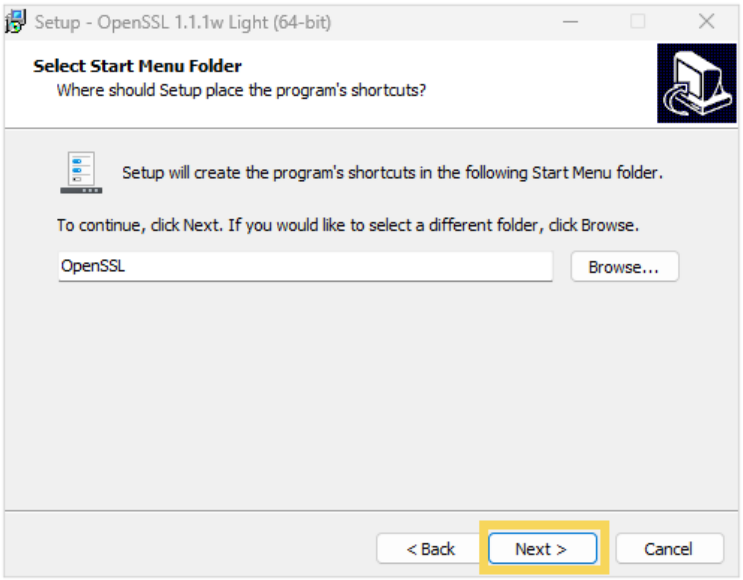


⑦インストール先のフォルダを指定して「Next」をクリックします。

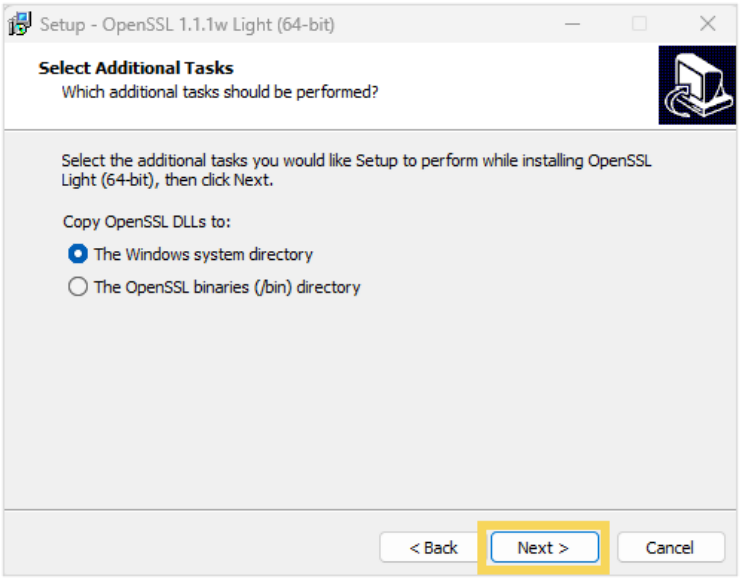
特に指定がなければデフォルトのフォルダのままクリックします。



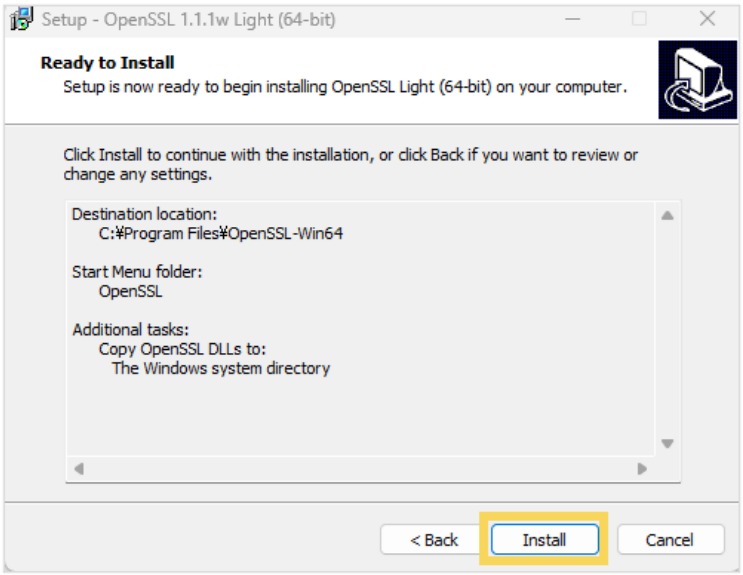
⑧「Next」をクリックします。



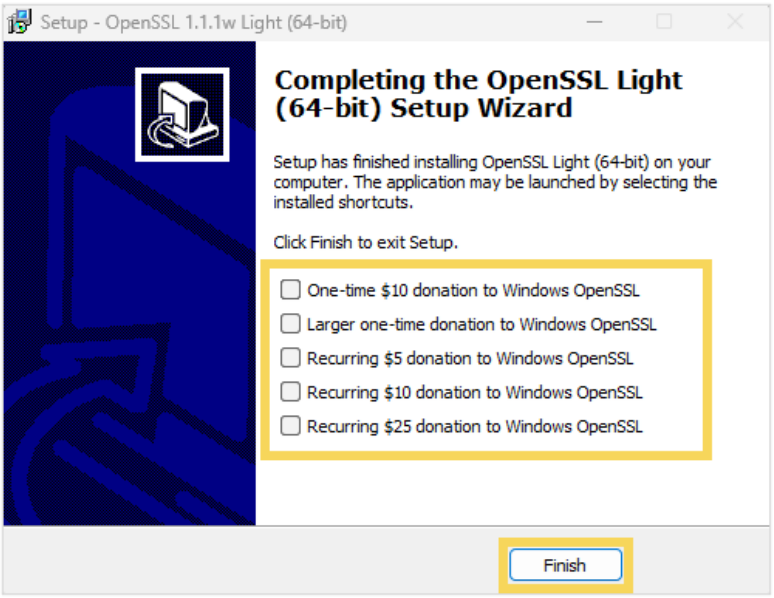
⑨「Next」をクリックします。



⑩「Install」をクリックします。

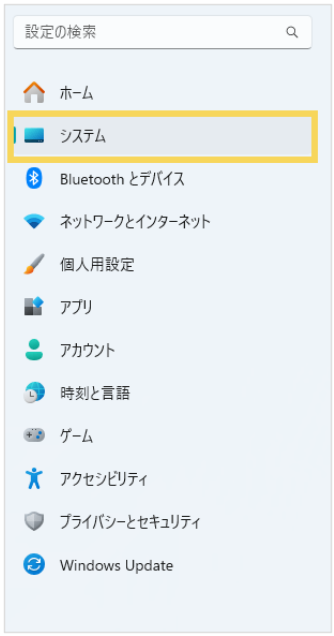


⑪すべてのチェックを外し、「Finish」をクリックします。

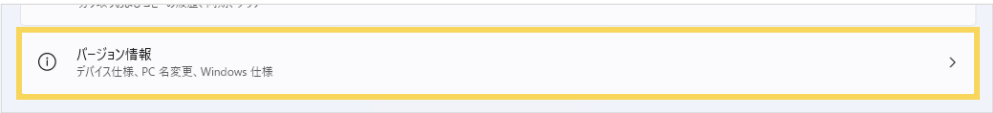


⑫Windows の「設定」をクリックします。

⑬「システム」をクリックします。



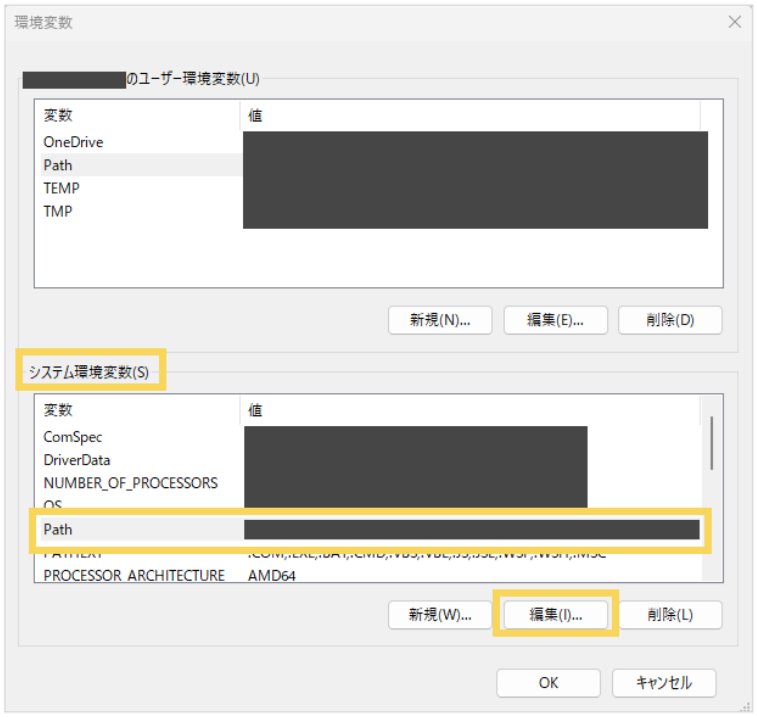
⑭「バージョン情報」をクリックします。



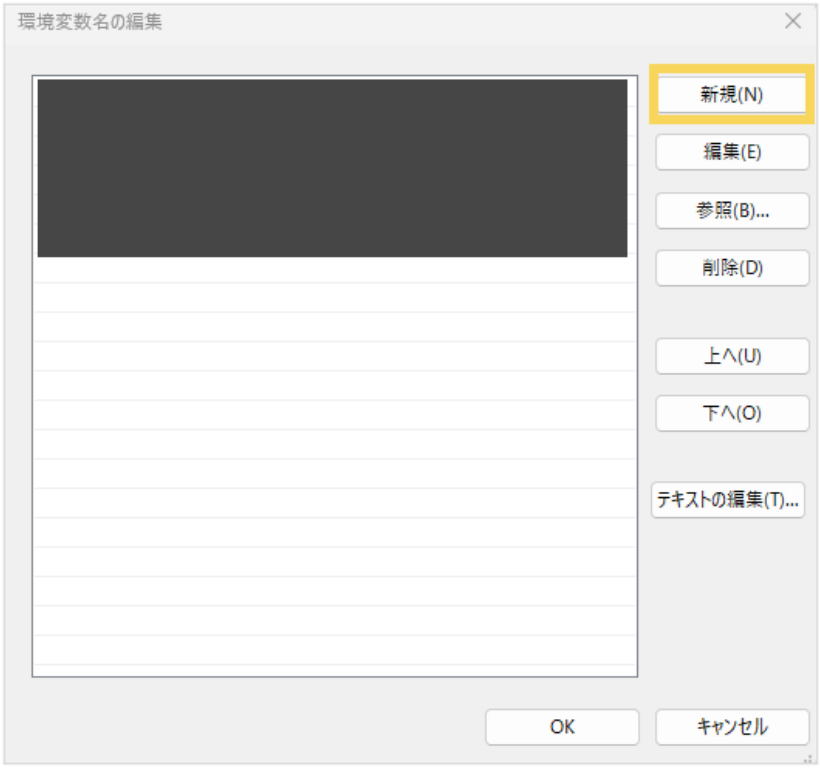
⑮「システムの詳細設定」をクリックします。

⑯「詳細設定」タブの「環境変数」をクリックします。

⑰「システム環境変数」の「Path」を選択し、「編集」をクリックします。

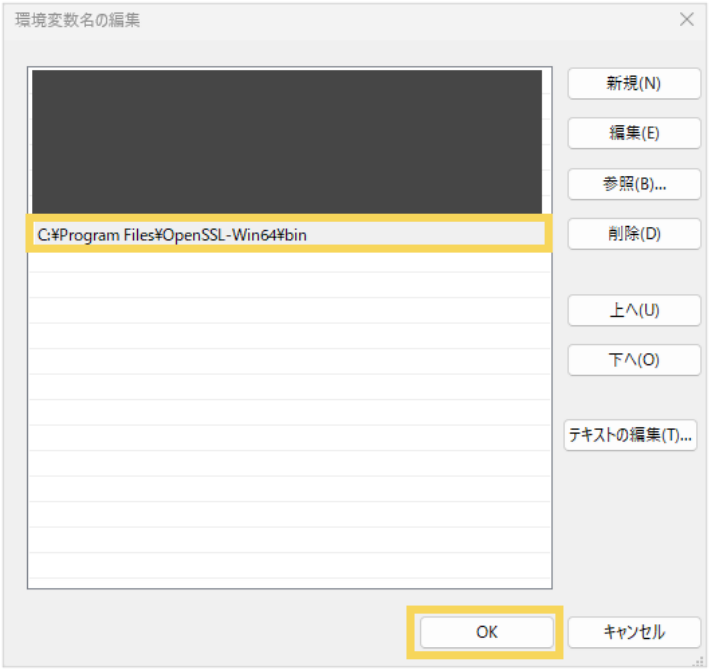


⑱「新規」をクリックします。



⑲OpenSSL をインストールしたフォルダを指定し、「OK」をクリックします。

手順⑦でデフォルトのフォルダを指定した場合は、「C:¥Program Files¥OpenSSL-Win64¥bin」と入力します。



⑳PC を再起動します。

※PC を再起動するまでは⑲で追加したシステム環境変数が適用されませんので、ご注意ください。

㉑再度「Windows Powershell」のアプリを起動します。

「openssl genpkey -out dkim.pem -algorithm RSA -pkeyopt rsa_keygen_bits:2048」と入力し、エンターキーを押します。

㉑「openssl rsa -in dkim.pem -pubout > dkim.pub」と入力し、エンターキーを押します。

㉒Windows のエクスプローラーを開き、「C:¥Users¥【ユーザー名】」のフォルダにアクセスします。

dkim.pem（秘密鍵）と dkim.pub（公開鍵）が格納されていれば、鍵ファイルの生成は完了です。

6.DKIM の設定確認方法

DKIM が正しく設定されているか確認する方法の一例として、外部サイトを利用した確認方法をご案内いたします。（※外部サイトの動作保証は致しかねますので、ご了承ください。）DKIM Record Checker – dmarcian（外部サイト）　https://dmarcian.com/dkim-inspector/

▼利用方法

①「Enter domain」エリアに貴社メールアドレスのドメインを入力

②「Enter selector」エリアに下記の作成者署名のセレクタを入力

※基本設定＞通知メール設定＞DKIM 設定＞「セレクタ」の設定内容を確認ください。

③「Inspect DKIM」ボタンをクリック

④チェック結果が表示されます。Your DKIM record is valid.と記載されていれば成功です。

エラー判定となってしまった場合は、今一度、サーバ管理者様（またはサーバ管理会社）へお問い合わせください。

7.DMARC の設定

■DMARC とは DMARC とは、SPF と DKIM を設定しているドメインからメールを送信した結果、メールの受信側サーバで送信元ドメインのなりすましやメール改ざんの疑いがあると判断されてしまった場合の対処法を指定する仕組みです。メールの送信者は、受信側がメールを拒否した場合に行う「破棄」「隔離（別の場所へ振り分けする）」「受信拒否」といった処理のうち、どの処理を行ってもらうかを指定できます。

受信側サーバでは DMARC の設定有無を元に迷惑メールの判定を行う場合がありますので、DMARC の設定を行うことで楽楽明細から送信されるメールが迷惑メールとして判断されにくくなります。
また、合わせて「SPF」「DMARC」の設定を行うことで、メールの到達率を向上させることができます。

■設定手順

【１】「お客様向けメールの From アドレス」を確認

管理画面　＞　基本設定　＞　通知メール設定画面　＞　「お客様向けメールの From アドレス」に設定されているメールアドレスを確認します。こちらのメールアドレスを運用（設定）しているサーバ管理者様（またはサーバ管理会社）を確認します。

【２】サーバ管理者様へ設定方法の確認・設定

【１】で確認したサーバ管理者様（またはサーバ管理会社）に、DMARC レコード（TXT 形式）の設定方法および記述方法を確認の上、DMARC 設定を行ってください。

※設定方法および記述形式はサーバ管理会社様により異なります。

8.DMARC の設定確認方法

DMARC が正しく設定されているか確認する方法の一例として、外部サイトを利用した確認方法をご案内いたします。（※外部サイトの動作保証は致しかねますので、ご了承ください）

CMARC Record Checker – dmarcian（外部サイト）

https://dmarcian.com/dmarc-inspector/

▼利用方法

①「Enter domain」エリアに貴社メールアドレスのドメインを入力

※「XXX@●●.co.jp」の場合、●●.co.jp を入力

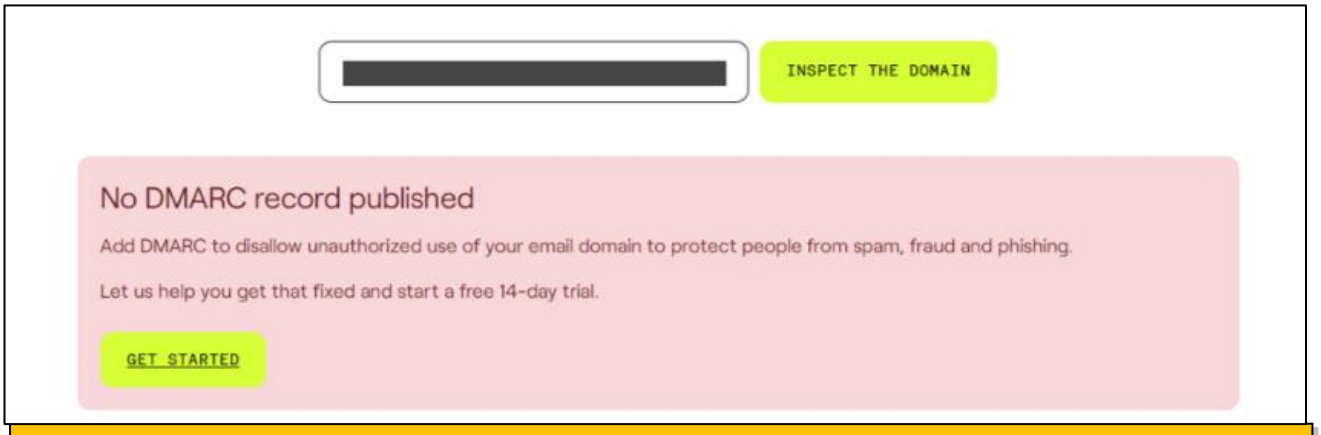
※@は含めない

②「INSPECT THE DOMAIN」をクリック

③チェック結果が表示されます。

CMARC 設定が有効になっていない場合は、「No DMARC record published」と表示されます。

失敗時（例）：



エラー判定となってしまった場合は、今一度、サーバ管理者様（またはサーバ管理会社）へお問い合わせください。※外部サイトのため画面イメージが変更になる場合がございます。予めご了承くださいませ。