## § HOME-UNIT3 の送受信メールに対する暗号化 対応について

HOME-UNIT3 では、SSL インスペクション機能を有効化することで、 SSL/TLS で暗号化されたメール通信に対してアンチウイルス検疫、ア ンチスパム検疫、添付ファイル自動 ZIP 暗号化機能、誤送信防止機 能を利用できます。ただし、ご利用にはクライアント端末への証明書の インポート作業やメーラの設定変更などの作業が必要です。 設定をご希望の場合には、HOME-CC にご相談ください。

また、証明書のインストールや各種設定作業はお客様ご自身で実施ください。

対応プロトコルや制限事項については、下記 URL からホワイトペーパ 「HOME-UNIT3 のセキュリティ機能について」も併せてご参照ください。

ホワイトペーパ: https://hmbx.canon.jp/agreement/index.php/wp-unit

※本機能を利用することでメール送受信や Web ブラウジングが多い 環境では、ネットワークの遅延等が発生する可能性あります。

# §メール送受信暗号化の対応(Windows)

1. 添付ファイル ZIP 暗号化機能、誤送信防止機能の (Windows)の動作環境

HOME-UNIT3のSSLインスペクション機能(メール送受信暗号化 (SSL/TLS)対応)は以下の環境での動作を確認しています。 下記以外の環境で本機能を利用する場合、デモ等の事前接続確 認を実施していただくことを強く推奨します。

Windows 10

- Windows 8.1
- メールソフト : Outlook (2013/2016)
- メールソフト: Thunderbird

※デモ等を利用した事前の動作確認を推奨します。 ※全てのアプリケーション、用途での動作を保証するものではありません。

## 2. 証明書のインストール (Windows + Outlook)

 以下の URL にアクセスし、ツール・アプリケーションからメール送 受信時暗号化対応に必要な SSL 証明書をダウンロードして ください。

HOME-UNIT4/3/2 管理者向けヘルプ https://hmbx.canon.jp/help9a/index.php/u nit2\_admin

 ダウンロードした ZIP ファイルを展開(解凍)し、証明書をダブ ルクリックしてください。



メール送受信暗号化(SSL/TLS)対応編

Ver1.6

③ 「セキュリティの警告」ウインドウが表示されますので、「開く」をクリ ックしてください。



④ 「全般」タブで、「証明書のインストール」をクリックしてください。

▲ 記 全形	E明書 2 詳細 証明	のパス	×
	証明書の相     この CA ルート証明書 明書を信頼されたル	青報 ■は信頼されていません。信頼を有 ■ト証明機関のストアにインストーノ	効にするにはこの証 してください。
		SAXA SSL Terminal CA 2019	
	発行者: 有効期間 20	SAXA SSL Terminal CA 2019 117/01/01 から 2037/01/01	
		証明書のインストール(I)	発行者のステートメント(S)
			ОК

⑤ 「ローカルコンピュータ」を選択し、「次へ」をクリックしてください。
 ※「次へ」クリック後に Windows の警告ウインドウが表示された場合は、「はい」をクリックしてください。

÷ \$	☞ 証明書のインポート ウイザード	×
	証明書のインボート ウィザードの開始	
	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リストをディスクから証明書ストアにコピー します。	
	証明機関によって発行された証明書は、ユーザーID を確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための信報を合んでいます。証明書ストアは、証明書が保管されるシステム 上の領域です。	
	保存場所	
	○現在のユーザー(C)	
	● ローカル コンピューター(L)	
	続行するには、 [次へ] をクリックしてください。	
	愛次へ(N)     キャンセル	ı

⑥ 「証明書をすべて次のストアに配置にする」を選択し、「参照」を クリックしてください。



⑦ 「信頼されたルート証明機関」を選択し、「OK」をクリックしてください。

※必ず「信頼されたルート証明機関」を選択してください。選択 しない場合、インストールした証明書が正しく機能しません。

証明書ストアの選択	×
使用する証明書ストアを選択してください(C)	
C <sup>O</sup> (P) (	
● 個人 ● 信頼されたルート証明機関	
ニニュー エンタープライズの信頼	
, — 中間証明機関	
□ 信頼されていない証明書 ○ サードパーティルート証明機関	
	•
□物理ストアを表示する(S)	
OK +72	セル

⑧ 「次へ」をクリックしてください。

		×
÷	証明書のインボート ウィザード	
	証明書ストア	
	証明書ストアは、証明書が保管されるシステム上の領域です。	
	Windows に証明音ストアを自動的に選択させるか、証明音の場所を指定することができます。	
	○ 証明書の種類に基づいて、自動的に証明書ストアを選択する(U)	
	④ 証明書をすべて次のストアに配置する(P)	
	証明書ストア:	
	信頼されたルート証明機関 参照(R)	
		-
	次へ(N) キャンセ	JL

⑨ 「完了」をクリックしてください。

証明書のインポート ウィザードの完了	
「中マ」をクリックオスと 証明書がインポートされます	
次の設定が指定されました:	
ユーザーが選択した証明書ストア 信頼されたルート証明機関	
内容 証明書	

① 「正しくインポートされました。」のポップアップが表示されましたら、 「OK」をクリックしてください。



 メールプロバイダの案内に従い、メールソフトの設定を変更してく ださい。

### 3. 証明書のインストール(Windows + Thunderbird)

 以下の URL にアクセスし、ツール・アプリケーションからメール送 受信時暗号化対応に必要な SSL 証明書をダウンロードして ください。

HOME-UNIT4/3/2 管理者向けヘルプ https://hmbx.canon.jp/help9a/index.php/unit2\_ admin

- ② Thunderbird を起動してください。
- ③ Thunderbird メニューバーで、[ツール]-[オプション]をクリックしてください。



④ 「詳細」タブを選択してください。



⑤ 「証明書」タブを選択してください。



⑥ 「証明書を管理」をクリックしてください。



⑦ 「認証局証明書」タブを選択し、「インポート」をクリックしてくださ



⑧ 手順①でダウンロードした証明書ファイルを選択し、「開く」をクリックしてください。



⑨ 以下の設定を行い、「OK」をクリックしてください。

項目	設定値
この認証局によるウェブサイトの識別を 信頼する	チェック
この認証局によるメールユーザーの識別を 信頼する	チェック



#### 10 「OK」をクリックしてください。

小しの11111日 日人11111日 9-1(-111-9)日 10-1111	A 100-23 Line	
認証局を識別するため以下の証明書が登録されてい	ξ <i>τ</i>	
証明書名と発行者名	セキュリティデバイス	
∨AC Camerfirma S.A.		
Chambers of Commerce Root - 2008	Builtin Object Token	
Global Chambersign Root - 2008	Builtin Object Token	
VAC Camerfirma SA CIF A82743287		
Camerfirma Chambers of Commerce Root	Builtin Object Token	
Camerfirma Global Chambersign Root	Builtin Object Token	
VACCV		
ACCVRAIZ1	Builtin Object Token	
∨Actalis S.p.A./03358520967	-	
キテのの 信頼性を設定(の) インボート	100 エクフポート/V) 削除すたけ信頼1 たい/D)	

### ① 「OK」をクリックしてください。

オプション								×
	<b>1</b> 表示	編集	チャット	ブライバシー	242J71	し 添付ファイル	カレンダー	К С
一般 データの	)選択 ネットワークと	ビディスク領域 更楽	f 証明書					
サーバーが作 〇 自	サーバーが個人証明書を表示したとき: ○ 自動的に選択する(3) ◎ 毎回自分で選択する(4)							
✓ OCSP	レスボンダーサーバー	こ問い合わせて証明	書の現在の正	E当性を確認する(C	ນ			
証明書を	管理(M) セキュ	リティデバイス( <u>D</u> )						
							ОК	キャンセル

② メールプロバイダの案内に従い、メールソフトの設定を変更してく ださい。

# §メール送受信暗号化の対応(Mac OS)

1. 添付ファイル ZIP 暗号化機能、誤送信防止機能の (Mac OS)の動作環境

HOME-UNIT3のSSLインスペクション機能(メール送受信暗号化 (SSL/TLS)対応)は以下の環境での動作を確認しています。 下記以外の環境で本機能を利用する場合、デモ等の事前接続確 認を実施していただくことを強く推奨します。

- Mac OS X v10.15 Catalina
- Mac OS X v10.14 Mojava
- Mac OS X v10.13 High Sierra
- Mac OS X v10.12 Sierra
- メールソフト: Mac 標準メールソフト

※デモ等を利用した事前の動作確認を推奨します。 ※全てのアプリケーション、用途での動作を保証するものではありません。

## 2. 証明書のインストール(MacOS+ 標準メールソフト)

 以下の URL にアクセスし、ツール・アプリケーションからメール送 受信時暗号化対応に必要な SSL 証明書をダウンロードして ください。

HOME-UNIT4/3/2 管理者向けヘルプ https://hmbx.canon.jp/help9a/index.php/unit2\_ admin

 ダウンロードした ZIP ファイルを展開(解凍)し、証明書をダブ ルクリックしてください。



③ 「証明書の追加」画面が表示されますので、「キーチェーン」を 「システム」に変更し、「追加」をクリックしてください。

000	証明書の追加
Centificate	ファイルやsynd 55L Certificate.CERからキーチェーンに証明書を追加 してもよるしいですか もいいートに開催し、際在のユーザのログインキーチェーンに追加されま す。このマシンをすべてのユーザによって証明書が共有される場合は、シス テムキーチェーンに追加されます。
証明書を表	キーチェーン・システム 📦

④ ユーザ認証を求められた場合、管理者のユーザ名、パスワード を入力し、「キーチェーンを変更」をクリックしてください。



⑤ キーチェーンアクセスの分類「すべての項目」をクリックして、ダウ ンロードした証明書を選択し、ダブルクリックしてください。

••• + (i)			
キーチェーン ● ログイン ● ローカル項目 ● システム ■ システム	Centificate         ルート該証局           パート         第3期限: 2037年1月11           ごのルート証明書は	nal CA 2019 日 木曜日 9時00分001 言頼されていません	沙 日本標準時
4	名前	~ 種類	変更日
	🖂 contactple burbaros icie	証明書	
	Comusipple iterberos kob	公開鍵	
	zonupple kerkens kau	秘密鍵	
	🔄 er er sample sy dre af din di	証明書	
	🔛 contacpie systemicia. I	証明書	
	P comuspie av stemd stault	公開鍵	
	P comuspie systemperault	公開鍵	
	💡 manaqqala systematistanil	秘密鍵	
分類	💡 contangés systemétria. B	秘密鍵	
金 すべての項目	SAXA SSL Terminal CA 2019	証明書	
1 137-5			
私家メモ			
自分の証明書			
() an			
6 Rec .			

⑥ 証明書の「信頼」をクリックし、「この証明書を使用するとき」を 「常に信頼」に変更してください。



⑦ ユーザ認証を求められた場合、管理者のユーザ名、パスワード を入力し、「設定をアップデート」をクリックしてください。



⑧ 証明書が追加されていることを確認し、ウインドウを閉じてください。

•••+•			
キーチェーン ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	Certificate していたいでは、 Certificate ののでのでは、 たいたいでは、 ののでのでのでは、 ののでのでので、 ののでので、 ののでので、 ののでので、 ののでので、 ののでので、 ののでので、 ののので、 のののので、 ののので、 のので、 のので、 ののので、 ののので、 のので のので	<b>hinal CA 2019</b> 1日 木曜日 9時00分00 てのユーザにとって信頼:	<b>9 日本標準時</b> されているものとして指定されています
	名前	~ 種類	変更日
	k ansteppietkarberustikie	証明書	
	💡 cara-apple.kerberas.lete	公開鍵	
	Province production in a matching	秘密鍵	
	Remains a pairs systematic healt	証明書	
	🔯 kom applausystemdefeult	証明書	
	Kansappieusystemdetault	公開鍵	
	§ canagainayetendelaak	公開鍵	
	Promo applicação en televil.	秘密鍵	
分類	© conseptions/standeleuk	秘密鍵	
→ すべての項目	SAXA SSL Terminal CA 2019	∋ 証明書	
/ パスワード		_	

⑨ メールプロバイダの案内に従い、メールソフトの設定を変更して ください。

## §メール送受信暗号化の対応(iOS)

1. 添付ファイル ZIP 暗号化機能、誤送信防止機能の (iOS)の動作環境

HOME-UNIT3のSSLインスペクション機能(メール送受信暗号化 (SSL/TLS)対応)は以下の環境での動作を確認しています。 下記以外の環境で本機能を利用する場合、デモ等の事前接続確 認を実施していただくことを強く推奨します。

- iOS 10
- iOS 11
- iOS 12
- iOS 13
- メールアプリ:iOS 標準メールアプリ

※デモ等を利用した事前の動作確認を推奨します。 ※全てのアプリケーション、用途での動作を保証するものではありません。

### 2. 証明書のインストール(iOS + 標準メールアプリ)

 以下のURLにアクセスし、ツール・アプリケーションからメール送受 信時暗号化対応に必要な SSL 証明書をダウンロードしてください。

> HOME-UNIT3/2 管理者向けヘルプ https://hmbx.canon.jp/help9a/index.php/unit2\_ admin

- ② ダウンロードした ZIP ファイルを展開(解凍)してください。
- 手順②で解凍した証明書ファイルをメールで iOS に送付してください。
- ④ iOS で、手順③で送付したメールを受信し、添付された証明書 をタップしてください。
- ⑤ 「インストール」をタップしてください。



⑥ 「警告」画面が表示されたら、「インストール」をタップしてください。



「インストール完了」画面が表示されたら、「完了」をタップしてください。



⑧ 「ホーム」画面で、「設定」アイコンをタップしてください。



⑨ 「一般」をタップしてください。



#### ⑩ 「情報」をタップしてください。



### ⑪ 「証明書信頼設定」をタップしてください。

く一般	情報
キャリア	
Wi-Fiアドレス	B-11721-1123
Bluetooth	5499375381964CC
IMEI	\$5.577104165-661 <sup>4</sup>
ICCID	6455 (19825)
MEID	3-515 -5-34
モデムファームウェア	5.53,61
SEID	>
法律に基づく情報	>
証明書信頼設定	>

② 「SAXA SSL Terminal CA 2019」を ON にしてください。



13 「続ける」をタップしてください。



 ④ 「SAXA SSL Terminal CA 2019」がON になっていることを 確認してください。



- 15 画面左上の「情報」をタップしてください。
- 16 画面左上の「一般」をタップしてください。
- 1 画面左上の「設定」をタップしてください。
- 18 「設定」画面を終了してください。

## §メール送受信暗号化の対応(Android)

1. 添付ファイル ZIP 暗号化機能、誤送信防止機能の (Android)の動作環境

HOME-UNIT3のSSLインスペクション機能(メール送受信暗号化 (SSL/TLS)対応)は以下の環境での動作を確認しています。 下記以外の環境で本機能を利用する場合、デモ等の事前接続確 認を実施していただくことを強く推奨します。

- Android 7
- Android 8
- Android 9
- Android 10
- メールソフト: Android 標準メールアプリ

※デモ等を利用した事前の動作確認を推奨します。 ※全てのアプリケーション、用途での動作を保証するものではありません。

- 証明書のインストール(Android + Android 標準メ
  - ールアプリ)
     ※本手順は、HUAWEI に搭載された、Android8.0.0 にて 作成しております。

機種、OS バージョンが異なる場合、画面表記等に差異がございます。詳細な画面表記、操作手順につきましては、各端末の メーカにご確認ください。

 PC で、以下の URL にアクセスし、ツール・アプリケーションからメ ール送受信時暗号化対応に必要な SSL 証明書をダウンロード してください。

> HOME-UNIT3/2 管理者向けヘルプ https://hmbx.canon.jp/help9a/index.php/unit2\_ admin

- ② ダウンロードした ZIP ファイルを展開 (解凍) してください。
- ③ 手順②で解凍した証明書ファイルをメールで Android に送付し てください。
- ④ Android で、手順③で送付したメールを受信し、添付された証明書をタップしてください。
- ⑤ 「証明書インストーラー」をタップしてください。



⑥ 「証明書名」に任意の名前を設定し、「OK」をタップしてください。



証明書名:	
UNIT3証明書	
認証情報の使用:	
VPNとアプリ	
パッケージの内容: 1個のCA証明書	
The state of the state	
キャンセル	OK

 ⑦ [設定]-[セキュリティとプライバシー]をタップし、「セキュリティとプラ イバシー」を表示してください。

設定			セキュリティとプライバシー	Q
	<b>アプリと通知</b> 相限、デフォルトアプリ		REAL PROPERTY CONTRACTOR REAL PROPERTY CANADA STREET	
۰	電池 省電力モード、電池消費量		HiSuiteのHDB許可を取り通し	
•	画面 長力保護、ホーム街面スタイル、登紙		ストレージタイプ ハードウェアサポート	
	音 通知の場影を開、首位百、バイブレーション		価額できる認証情報 伝報できるCA証明者を表示する	
	ストレージ メモリ、ストレージクリーナー		ユーザー認証情報 保存されている認証情報の表示と変更	
•	セキュリティとプライバシー ■ボロックとパスワード	>	SDカードからインストール 証明書を50カードからインストールする	
0	アカウント	- 51	認証ストレージの消去 証明書をすべて消去する	

#### ⑧ 「信頼できる認証情報」をタップしてください。

設定		セキュリティとプライバシー	Q
	<b>アプリと通知</b> 相思、デフォルトアプリ	BT.	-
۰	電池 省電力モード、電池消費量	HiSuiteのHDB許可を取り消し	
	画面 初力保護、ホーム面面スタイル、望紙	ストレージタイプ ハードウェアサポート	
	音 通知の視動利限、著信言、バイブレーション	信頼できる認証情報 伝報できるCA証明書を表示する	×
	ストレージ メモリ、ストレージクリーナー	ユーザー認証情報 保存されている認識情報の表示と変更	
0	セキュリティとプライバシー 画面ロックとパスワード	SDカードからインストール 証明書をSDカードからインストールする	
Ø	アカウント	認証ストレージの消去 証明書をすべて満去する	

 「ユーザー」をタップし、「SAXA SSL Terminal CA 2019」が あることを確認してください。

システム	ユーザー
SAXA SAXA SSL Terminal CA 2019	
信頼できる認証情報	

●Canon、iR はキヤノン株式会社の商標です。

•Mac OS は米国 Apple Computer, Inc.の商標です。

•Microsoft、Windows、Windows 8.1/10、Exchange、Microsoft OFFICE、 Internet Explorer は、米国 Microsoft Corporation の米国およびその他 の国における登録商標または商標です。

•Android は、Google Inc.の商標または登録商標です。

•iPhone、iPad、Multi-Touch は Apple Inc.の商標です。

•Firefox は、米国 Mozilla Foundation の米国及びその他の国における 商標または登録商標です。

•その他記載されている会社名、製品名等は、該当する各社の商標または 登録商標です。

ご不明な点がありましたら、 HOME コンタクトセンター (フリーダイヤル) 0120-188089 まで、お問い合わせください。

