JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

～ BIG-IP Edge Gateway & VMware View ～

クライアント証明書を用いたVPNおよび、仮想デスクトップへのシングルサインオン設定（PC／シンクライアント）

Ver.1.0

2012 年 10 月

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

・ JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
・ その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
・ Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

目次

1. はじめに

1.1. 本書について

本書では、弊社製品「プライベート CA Gléas」で発行したクライアント証明書を用いて F5 ネットワークス社製 SSL-VPN 装置「BIG-IP Edge Gateway」で VPN を張り、その認証情報を用いてヴイエムウェア社製仮想デスクトップインフラストラクチャー「VMware View」に対し、シングルサインオンをおこなう環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までご連絡ください。

1.2. 本書における環境

本書における手順は、以下の環境で動作確認を行っています。

- 【VPN機器】BIG-IP Edge Gateway（バージョン11.1.0 build 1943.0）
  ※以後、「BIG-IP」と記載します
- 【仮想デスクトップ インフラストラクチャ】VMware View 5
  ※以後、「VMware」と記載します
  ※構成コンポーネントは以下の通りです
  ハイパーバイザー：VMware ESXi 5.0.0
  vCenterサーバ：Windows Server 2008 R2 Standard / vCenter Server 5.0
  View接続サーバ：Windows Server 2008 R2 Standard / View Connection Server 5.0
- 【ドメインコントローラ】Windows Server 2008 R2 Standard
  ※以後、「ドメインコントローラ」と記載します
- 【認証局】JS3 プライベートCA Gléas （バージョン1.10）
  ※以後、「Gléas」と記載します
- 【クライアントPC】
  Windows 7 Professional SP1 / VMware View Client 5.2.0 build-848202
  ※以後、「PC」と記載します
- 【シンクライアント】日本HP 6360t Mobile Thin Client

Windows Embedded Standard 7 SP1 / VMware View Client 4.6.0 build366101

※以後、「シンクライアント」と記載します

以下については、本書では説明を割愛します。

- BIG-IPのVPN接続設定・クライアント証明書による認証設定

  ※弊社のWEBサイトでは、BIG-IPでのクライアント証明書認証をおこなうための環境構築のホワイトペーパーを公開しておりますので、構築時の参考にしてください

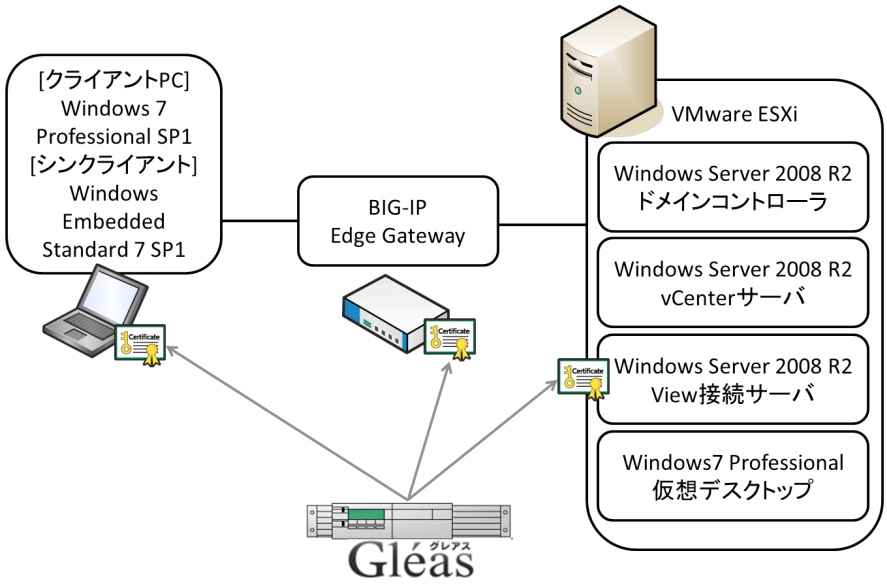
  参考URL：http://www.jcch-sss.com/service/support/2011/02/big-ip-ssl-client-auth
- VMware Viewでの仮想デスクトップインフラ環境の構築

  ※Windowsドメインでのユーザ ID／パスワードを用いてView接続サーバにログインし、仮想デスクトップを利用できる状態になっていることを前提としています
- Gléasでのユーザ登録やクライアント証明書発行等の基本設定
- PC・シンクライアントでのネットワーク設定等の基本設定

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



1. Viewクライアントはすでに PC・シンクライアントにインストールされているものとする。またBIG-IPに対するSSLサーバ証明書もすでにインストールされているものとする。

2. View接続サーバにサーバ証明書をインストールする
3. PC・シンクライアントには、Gléasより発行されたクライアント証明書をインポートする
4. PC・シンクライアントはBIG-IPに接続する。BIG-IPではクライアント証明書認証をおこない、さらに二因子認証として、Windowsドメインでのユーザ認証（パスワード認証）をおこなうが、この時のユーザIDはクライアント証明書のサブジェクトcn（一般名）から抽出する
5. 認証成功後SSL-VPNセッションが確立される。その後、Viewクライアントが自動的に起動しView接続サーバへの認証がおこなわれ仮想デスクトップが起動する

1.4. 電子証明書の発行時における留意事項

本環境で利用するクライアント証明書をGléasで発行する際には、以下の点に留意する必要があります。

- Gléasでのユーザアカウント（＝証明書サブジェクトのcn）と、Active Directoryでのユーザ名は同一にする必要があります
  ※Gléasでは、Active Directoryからアカウント情報をインポートさせることも可能です。詳細は弊社までお問い合わせください。

2. View接続サーバの設定

2.1. サーバ証明書のインポート

Gléasよりサーバ証明書ファイルをダウンロードします。
そのファイル（*.p12）をView接続サーバの以下のフォルダに配置します。
C:¥Program Files¥VMware¥VMware View¥Server¥sslgateway¥conf¥
（インストール先をデフォルトの場所より変えている場合は、適宜変更してください）

同フォルダにある locked.properties ファイルに以下を記述します。
（locked.properties が存在しない場合は、メモ帳などで新規作成します）

```
keyfile=[サーバ証明書ファイルのファイル名（*.p12）]
keypass=[Gléasから上記ファイルをダウンロードした時に設定したパスワード]
```

VMware View Connection Server サービスを再起動すると、設定が反映されます。
この時、ログファイルに以下のようなログが記録されます。
※ログファイルは以下にあります（デフォルトインストール時）

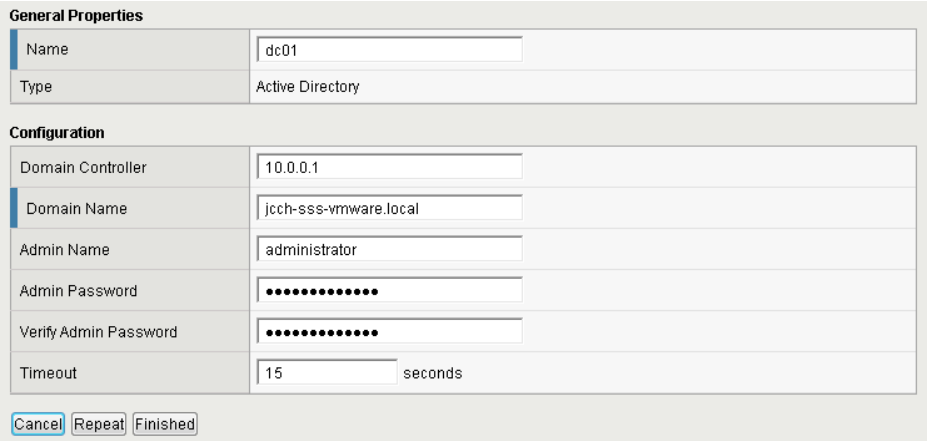
C:¥ProgramData¥VMware¥VDM¥logs

```
INFO <Thread-1> [q] The Secure Gateway Server is using SSL certificate store
filename.p12 with password of x characters
INFO <Thread-1> [q] The Secure Gateway Server is listening on https://*:443
```

3. BIG-IPの管理設定

3.1. Active Directory の登録

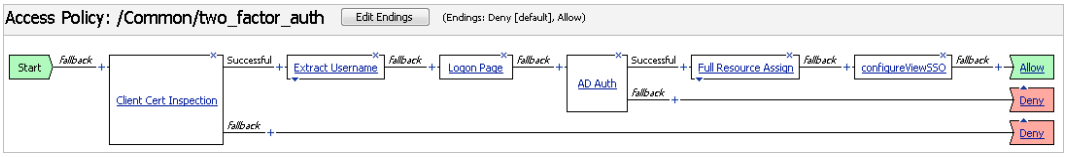
左ペインで[Access Policy] > [Access Profile] > [AAA Server] > [Active Directory]を選択し、右画面で[Create…]をクリックします。
ドメインコントローラに認証アクセスするための情報を設定します。



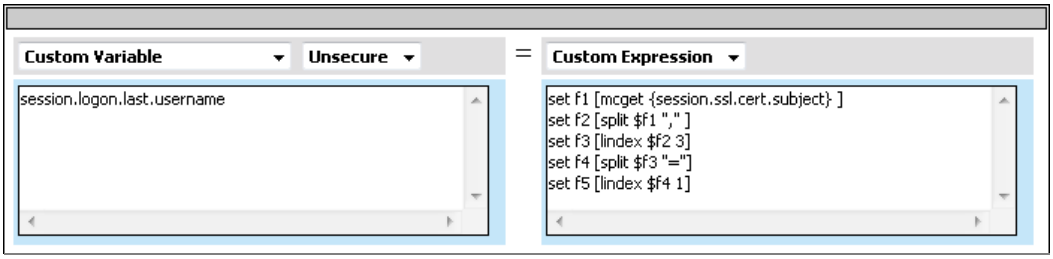
3.2. アクセスプロファイルの作成

左ペインで[Access Policy] > [Access Profile]と進み、右側画面で設定をおこなうアクセスプロファイルの[Edit…]をクリックし（あるいは[Create…]ボタンをクリックし新規作成）、ビジュアルポリシーエディター（VPE）を開きます。
※許可するクライアントなどのその他の接続条件は、必要に応じて追加してください

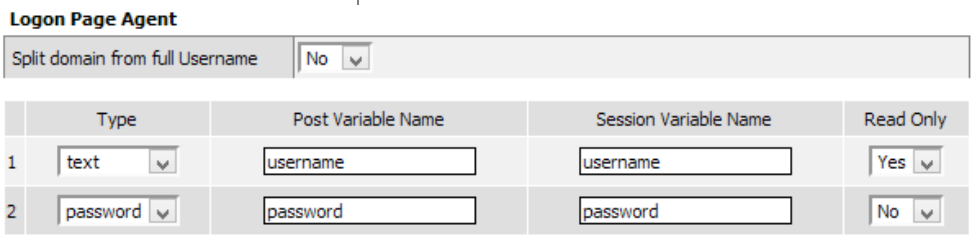
VPE でアクセスポリシーを設定します。以下は今回の設定例となります。
※VPE の操作方法については、本書では省略します
※許可するクライアントなどその他の接続条件は、必要に応じて追加してください



Client Cert Inspection	Branch Rule で、クライアント SSL プロファイルで設定されたクライアント証明書認証の結果をチェックします（デフォルトのまま）。
Variable Assign ※上図では”Extract Username”という名前に設定	カスタム変数 session.logon.last.username に証明書サブジェクト cn 値を代入するように設定します。 ※下図ではクライアント証明書のサブジェクトが dc=com, dc=example, ou=sales, cn=username のように cn が 4 番目（固定）であることを想定。この並び順により Custom Expression の 3 行目の”lindex $f2 3”の右側の”3”を変更する必要があります

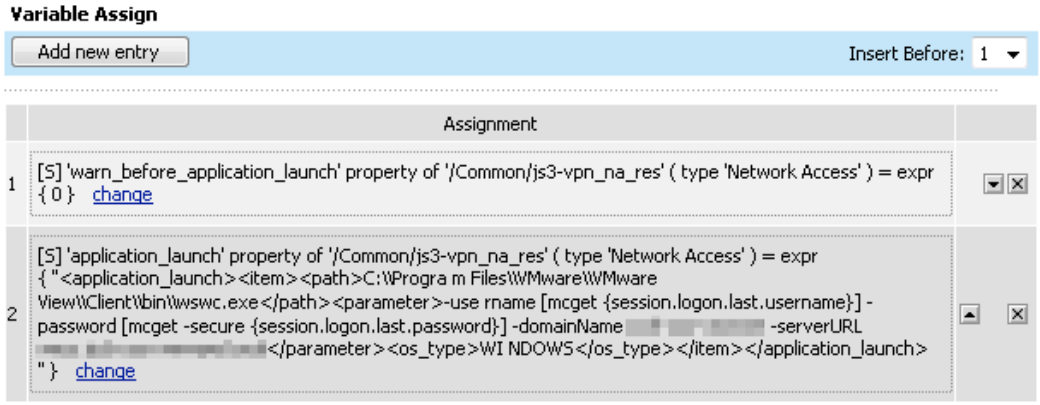


Logon Page	ユーザ ID はすでに取得しているので、Read Only を[Yes]に変更し変更不可に設定して、パスワードのみを入力させるよう設定します。

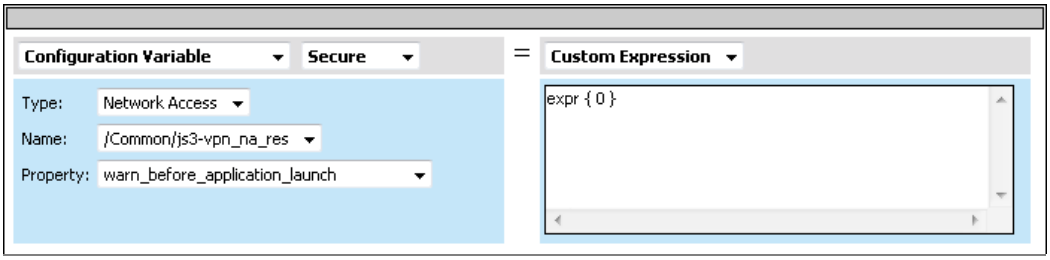


AD Auth	[Server]には 3.1 項で設定した Active Directory を設定します。 Branch Rule では、認証結果をチェックします（デフォルトのまま）
Full Resource Assign	設定済みのネットワークアクセスリソースと、Webtop を指定します。
Variable Assign	PC にインストールされた View クライアントを起動させま

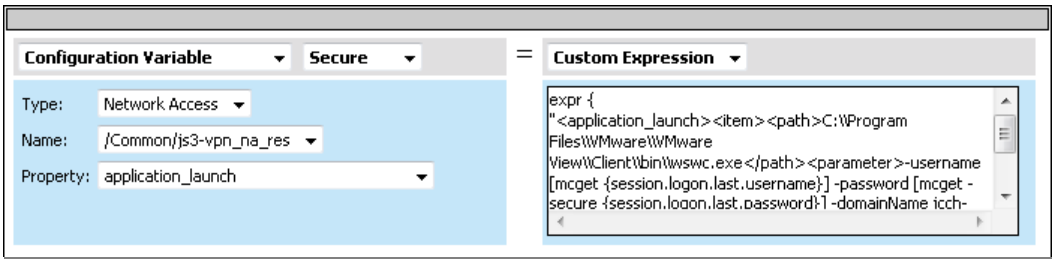
※上図では”configureViewSSO”という名前に設定	す。 1 行目は、アプリケーション起動時の警告を出現させない設定です。2 行目は、View クライアントの起動設定になります。



（1 行目）



（2 行目）



上図右側の内容は以下の通りです。

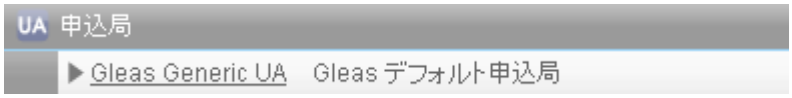
```
expr {
"<application_launch><item><path>C:¥¥Program Files¥¥VMware¥¥VMware
View¥¥Client¥¥bin¥¥wswc.exe</path><parameter>-username [mcget
{session.logon.last.username}] -password [mcget -secure
{session.logon.last.password}] -domainName [ドメイン名] -serverURL [View 接続サーバの
FQDN]
-unattended</parameter><os_type>WINDOWS</os_type></item></application_launch>" }
```

※View クライアントがカスタムロケーションにインストールされている場合は、正しいパス設定する必要があります

※パラメータ「-unattended」を外すと、View クライアントでのログイン後に仮想デスクトップ選択画面が表示されるようになります

4. Gléasの管理者設定（PC）

GléasのRA（登録局）にログインし、画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定をおこなうUA（申込局）をクリックします。



[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [証明書ストアへのインポート]をチェック
- [証明書ストアの選択]で[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック

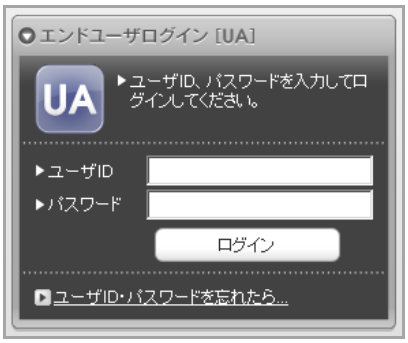
設定終了後、[保存]をクリックし設定を保存します。
各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

5. クライアント証明書を用いた VPN 接続

5.1. Gléas の UA からのクライアント証明書インストール

Internet ExplorerでGléasのUAサイトにアクセスします。
ログイン画面が表示されるので、ユーザIDとパスワードを入力しログインします。



ログインすると、ユーザ専用ページが表示されます。
初回ログインの際は、ActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。
その後、 [証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。

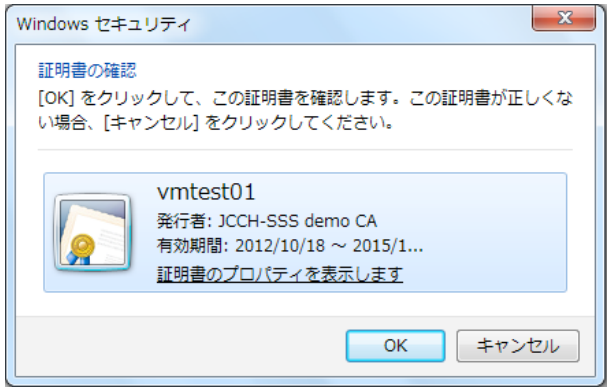
※「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません

5.2. VPN アクセス、および仮想デスクトップの利用

Internet ExplorerでBIG-IPへアクセスします。
PCにインポートされたクライアント証明書による認証（端末認証）と、Active Directory認証（ユーザ認証）を経て、Viewクライアントによる仮想デスクトップへ

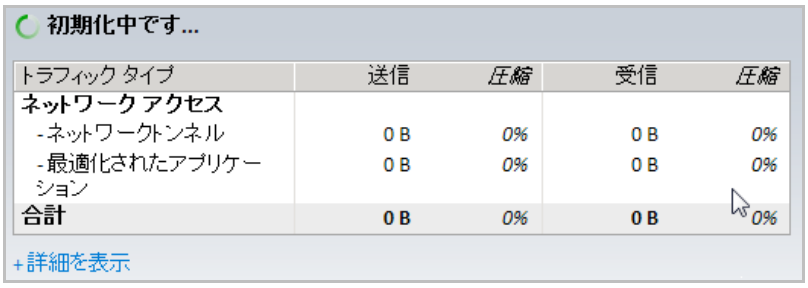
の自動接続がおこなわれます。

認証から仮想デスクトップへの流れは以下のとおりです。

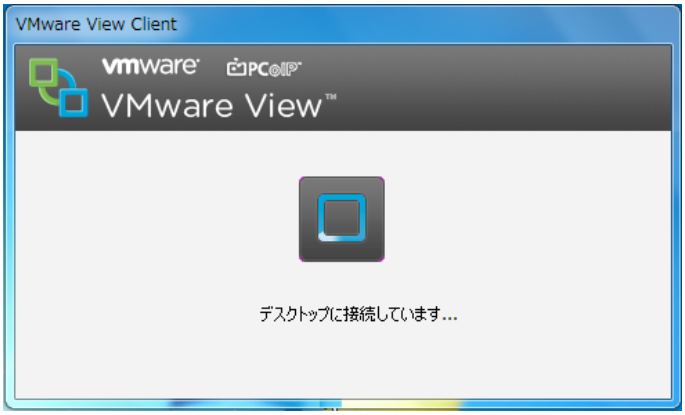


クライアント証明書認証（証明書選択ダイアログ）

BIG-IPでのユーザ認証画面（ユーザー名は証明書より抽出されているのでグレーアウトされています）



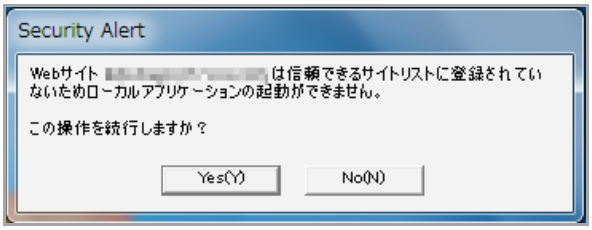
VPNトンネリング（Edge Clientコンポーネント）起動中画面



Viewクライアントの自動起動、及び仮想デスクトップへの自動接続

※3.2項のconfigureViewSSOの2行目のViewクライアントの起動パラメータの設定で、-unattendedを付加すると自動的に仮想デスクトップへの接続までおこなわれます（ユーザに割り当てられた仮想デスクトップが複数ある場合の挙動は弊社未検証）。

※BIG-IPのFQDNがInternet Explorerでの[信頼するサイト]に登録されていない場合（下図）や、UAC（ユーザのアクセス制御）がオンになっている場合などは、自動起動時にセキュリティ確認画面が出現します



6. シンクライアントでの接続設定

シンクライアントでは、Administratorでログインし EWF（Enhanced Write Filter）をオフにしてから以下の設定をおこないます。

（以下は、Userでログイン（デフォルト）しての操作です）

- クライアント証明書のインストール（Userでログイン）

  5.1項のとおりUAからインポートするか、RAよりダウンロードした証明書ファイル（*.p12）をダブルクリックすると起動するウィザードでインポートする方法があります

- BIG-IP Edge Client Components（VPNクライアントモジュール）のインストール

  BIG-IPへの初回アクセス時にインストールを促されるので、インストールします

- [信頼するサイト]への登録や、必要に応じUACの設定変更（Administratorでのログインが必要）をします

以上の設定が終わったら、EWFを有効にして5.2項のとおり接続をおこないます。

7. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■BIG-IPに関するお問い合わせ先

F5ネットワークスジャパン株式会社

Tel: 03-5114-3210

URL：http://www.f5networks.co.jp/fc

（上記URLのお問い合わせフォームよりご連絡ください。）

■VMware Viewに関するお問い合わせ先

ヴイエムウェア株式会社

URL：http://www.vmware.com/jp/company/contact.html

■シンクライアントに関するお問い合わせ先

日本ヒューレット・パッカード株式会社

プリンティング&パーソナルシステムズ事業統括

クライアントソリューション本部　製品部

Mail：thinclient.jpn@hp.com

■Gléasや検証用の証明書に関するお問い合わせ先

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel:　　050-3821-2195

Mail：sales@jcch-sss.com