Ver1.1(2020/9/10)

SmartSecret
オンデマンド
VPN

SSOV
(SS OnDemand VPN)

HunsLab Inc.

HunsLaB

目次

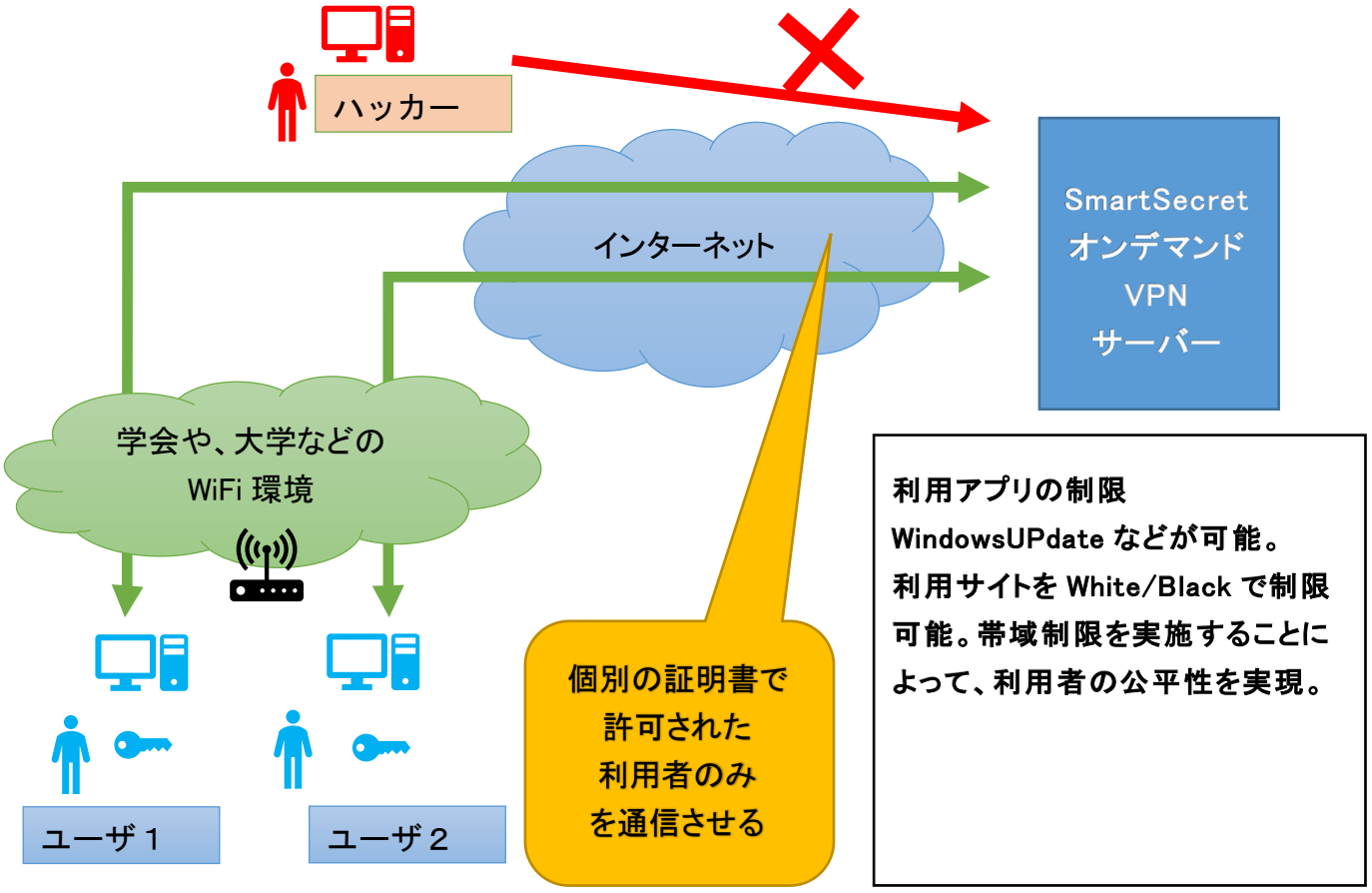
利用形態　（SS オンデマンド VPN アクセスサービス）

セミナー、学術会議、EXPO、フリーWiFi やホテルなどで提供される有線インターネットなどで提供されるインターネット接続環境には様々なリスクが存在します。

接続した WiFi 環境や有線環境では、安全な DNS を利用していない場合があり、悪意のあるサイトに誘導されるリスクがあります。またハッカーが同じネットワークに接続すると利用しているパソコンの脆弱性を攻撃され、重要な情報が漏洩するインシデントが発生しています。

国内、また海外など、どのような WiFi 環境、また有線環境をご利用いただいても、安全なインターネット接続を個別証明書ベースで実施することができるようになります。

SmartSecret オンデマンド VPN(SOV)接続では、接続環境として専用サーバまたは仮想サーバをクラウドに自動配置し、VPN アクセスサービスを利用できるサービス形態となります。



サーバはクラウドに構成されます。利用されるユーザ数、同時接続数、ご利用期間に応じて、クラウド環境を整備し、オンデマンドに応じて利用できるサービスとなります。

SmartSecret オンデマンド VPN ス(SOV)接続では、利用者ごとに個別証明書を配布する最も厳格な証明書管理を実現しています。

個別証明書に基づいて接続検証を行うため、パスワード接続や共通の証明書などに比べ、次元の異なる安全性を提供します。接続する利用者の通信の盗聴、証明書詐称攻撃（中間者攻撃）を排除します。

安全ではない、WiFi 環境においては、利用するパソコンの FW 機能を有効にすることが重要です。それは、SOV に接続されるまでは、攻撃の対象になるからです。

自動で接続する機能もご提供していますので、ご利用期間中は自動接続モードを推奨します。

証明書の配布方法、無効方法

ユーザへの証明書配布から利用までの流れは以下のように非常に簡単です。

① ユーザにダウンロード用の URL をメールで通知します。
② ユーザは URL を開き自分のメールアカウントを登録します。
③ 送信されてきたメールの URL を開き送付された情報でログインします。
④ パソコンやタブレットなどに証明書をインストールします。

管理者には誰が登録を終えたか、また接続しているかなどを WEB 管理画面から確認することが可能です。

利用登録するメールアカウントで利用するドメイン名の制限をかけることも可能です。
例）gmail.com のみなど

証明書を無効にすることで、利用者単位で使用を停止することが可能です。
発行した証明書を無効にすることが Web 管理画面で行えます。

また別途 API で証明書を発行、利用を停止、再開などする事が可能です。
例えば、事前に台数分を発行し、それをメールなどで配布する事が可能になります。

これによって既存のシステムとの自動連携などを自由に設計する事も可能です。
またアクティブディレクトリー(AD)との連携オプションもご用意しています。

利用においてもっとも重要なことは、
　ユーザにどのような方法で、証明書を配布すれば良いのか？
ということです。

利用させたいユーザに利用していただく事が最も重要なことです。

本人を確認する方法などについて、別途コンサルティングオプションもご用意しております。ぜひご利用ください。

サーバ SPEC と負荷分散、障害許容設計

クラウド接続用サーバは、物理サーバ、もしくは仮想サーバがご利用いただけます。

接続アカウント数 250 台当たり、

CPU	2Core 以上
Memory	4GB 以上
SSD	100GB 以上
NIC	2 ポート以上　Gigabit 以上 （DMZ もしくはポートフォワードの場合は 1 ポートで可能）

接続アカウントが多い場合、また接続サーバの信頼性向上のため、サーバを追加し、フォールトトレラント設計(障害許容設計)を行う事が可能です。

その際クライアント側では、故障時に自動で再接続を行います。
（クライアントは再接続した時点で、自動で復旧したサーバにも負荷分散します）

また、利用者が多くなり、クラウド側の SOV サーバーを増設することや、SSOV サーバーにリアルタイムで CPU やメモリー、回線スピードなどの増設が行えるサービスもご利用いただけます。

どちらのケースでも切り替えのダウンタイムは発生しません。

利用可能なクライアントデバイス

接続可能クライアント

IOS iPhone,iPad,
Windows7,8,10, タブレット版
MacOS X 10.x 以上
Linux（Ubuntsu,CentOS など）
Android Version7 以降を推奨
KindleOS
ChromeBook

利用可能クラウド環境

以下の構成から選択できます。
利用期間と利用人数、同時接続数、必要な帯域の情報から下記構成をデザイン致します。

1. 固定料金モデル：

利用するクラウド環境の例
さくらインターネット
お名前ドットコムなど

利用するユーザ数に制限はありません。
利用料金は固定料金となります。
利用期間は 1 日から可能です。
少ない利用者でご利用の場合は、従量課金モデルより高額になる場合があります。

2. 従量課金モデル：

利用するクラウド環境
AWS(アマゾン・ウェブ・サービス)
GCP(グーグル・クラウド・プラットフォーム)など

利用するユーザ数に制限はありません。
ただし、利用料金は従量課金となります。
利用期間は 1 日から可能です。
少ない利用者でご利用の場合は、固定料金モデルより低額になる場合があります。

海外でのご利用

本クライアントソフトウェアは海外でご利用が可能です。ご利用にあたって、
ユーザ様のご要望に合わせて輸出非該当証明書を無料で発行させていただきます。

株式会社 HUNS 研究所

輸出用非該当証明書

SmartSecretVPN

SmartSecretVPN を書き込んだ CD-R 等のメディア、またはインストールしたハードウェア（コンピュータなど）を物理的に日本国外に輸出する場合において日本政府の許可が必要であるかどうかが問題となります。通常、暗号装置を日本国外に輸出される場合は経済産業省の許可を個別に得る必要があります。しかし、SmartSecretVPN は貨物等省令第 8 条第九号タに定める装置であることが確認されていますので、輸出にあたり個別に許可を得る必要はありません。輸出時に SmartSecretVPN を書き込んだ CD-R 等のメディア、またはインストールしたハードウェア（コンピュータなど）について日本国の税関で「非該当証明書」の提示が求められた場合は、下記証明書を提示いただければ輸出できます。

SmartSecretVPN はアプリケーションプログラムです。その中では暗号技術を利用しますが、独自技術ではありません。稼働環境であるマイクロソフト社の Windows、アップル社の IOS の非該当証明書も携帯することをお勧めします。