Ver1.1(2020/4/10)

SmartSecret
セキュアリモートアクセス

SSRA
(SS Secure Remote)

HunsLab Inc.

HunsLaB

目次

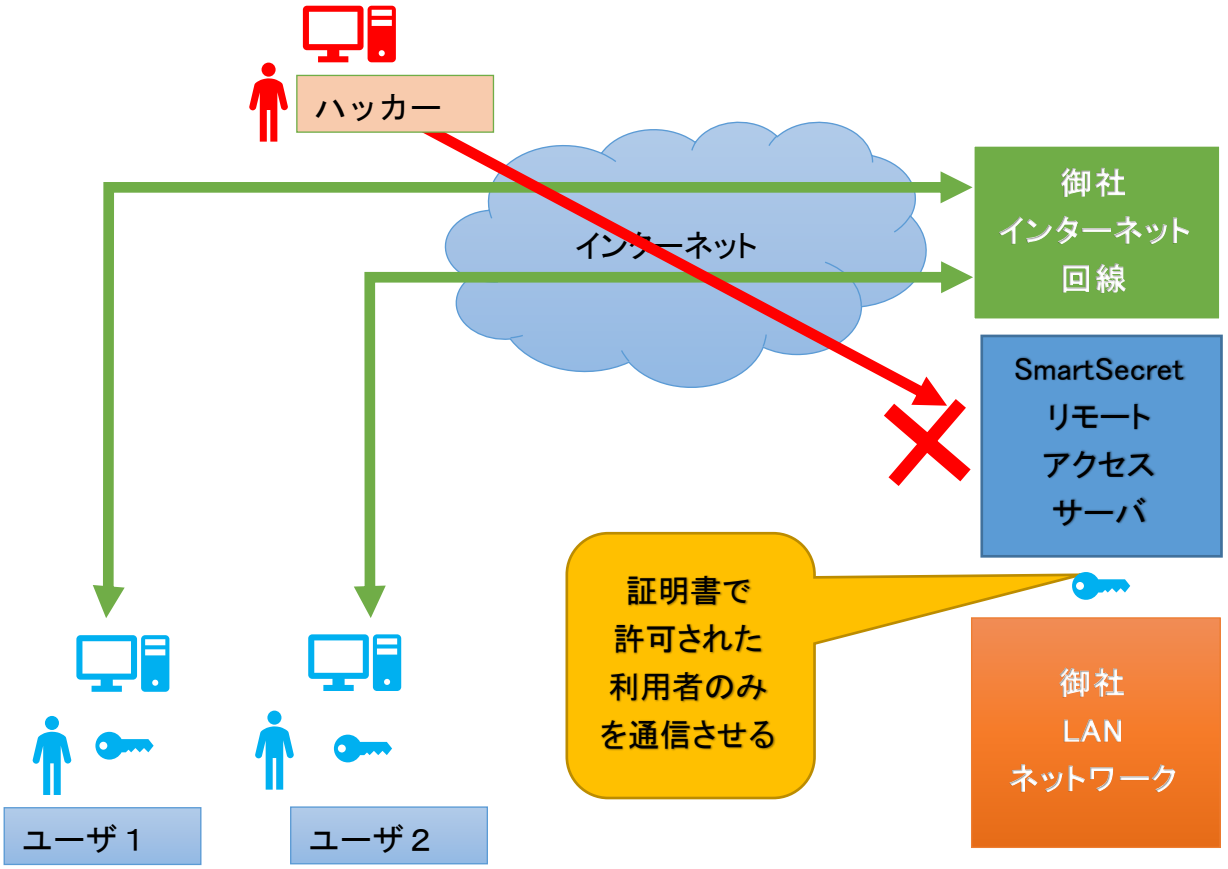
利用形態　（セキュアリモート接続）

SmartSecret セキュアリモート接続(SSRA)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お客様内に配置し、本ソフトウェアを導入しご利用いただく形態となります。

サーバはインターネット側と LAN 側に接続できる構成が必要となります。
(SSRA サーバの配置は DMZ もしくはポートフォワード方式が簡単です。この場合はネットワークは LAN 側のみで可能です。別途配置の構成図)

インターネット側としては、既存のインターネット回線をご利用いただく方法と、別途推奨インターネット回線をご利用いただく方法が選択できます。

SSRA はサーバソフトウェアとクライアントソフトウェアで構成されます。稼働させるサーバのセットアップ時には環境構築オプションをご利用いただけます。また、こちらで適正のあるハードウェアの代理購入なども承ります。

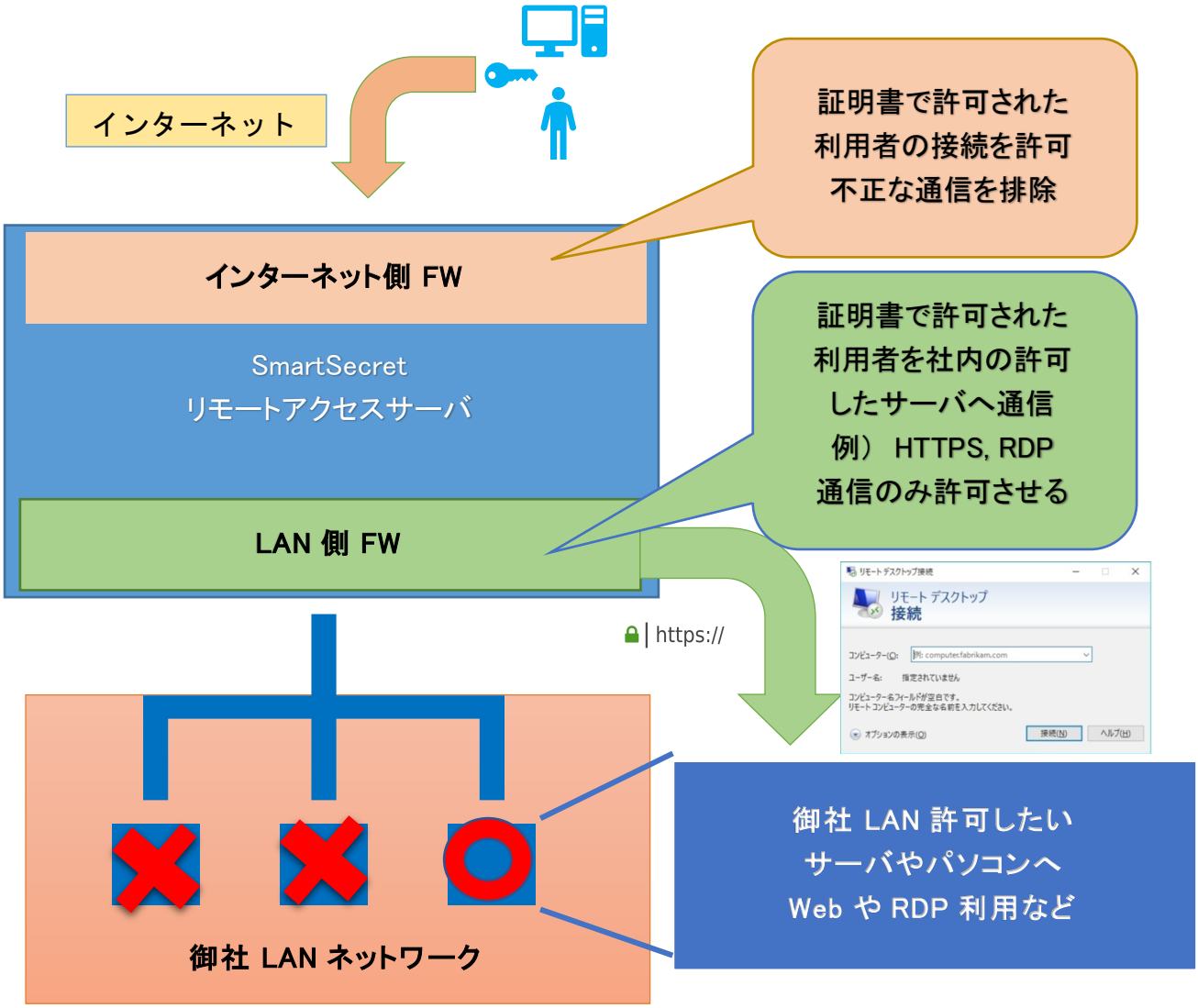


セキュリティポリシー

SmartSecret リモートアクセス(SSRA)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。

また接続されるユーザの LAN ネットワークへのアクセスを限定することが可能です。許可された Web サーバやリモートデスクトップ先のパソコンなどに許可されたプロトコルのみを通信させる事でリスクを排除します。



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。

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

社内に配置する接続用サーバは、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、リモートアクセス用の回線を施設した場合において、その回線への切り替えのダウンタイムも 10-30 分程度（切り替え前には事前に検証実施）で行えます。またその際に既に利用者に配布した証明書の変更作業などは一切ありません。

利用可能なクライアントデバイス

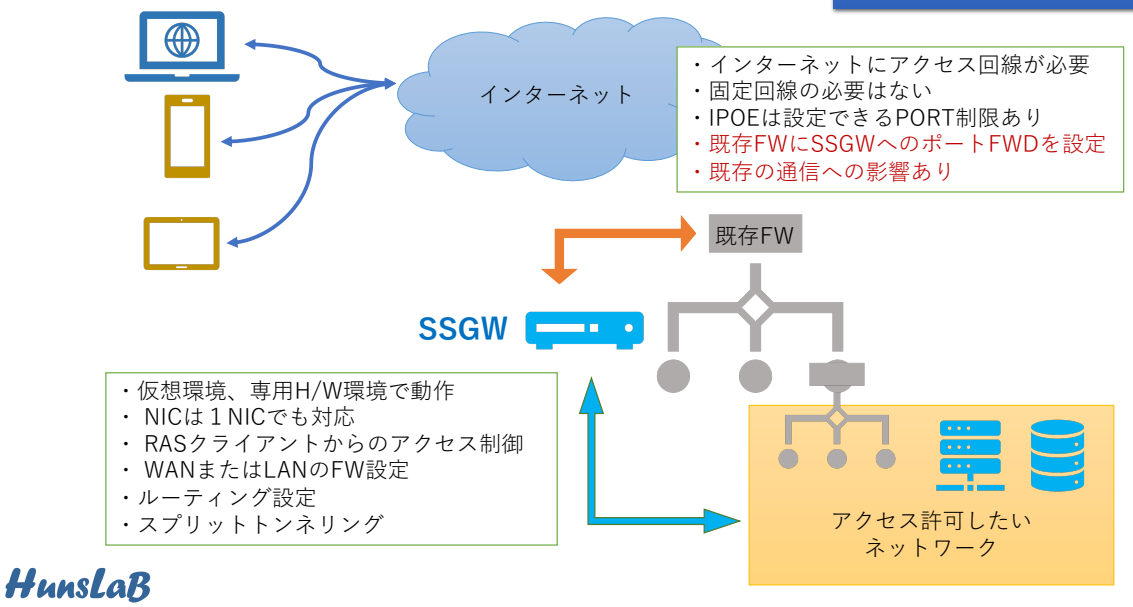
接続可能クライアント

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

接続構成の例

設置ユースケースその①

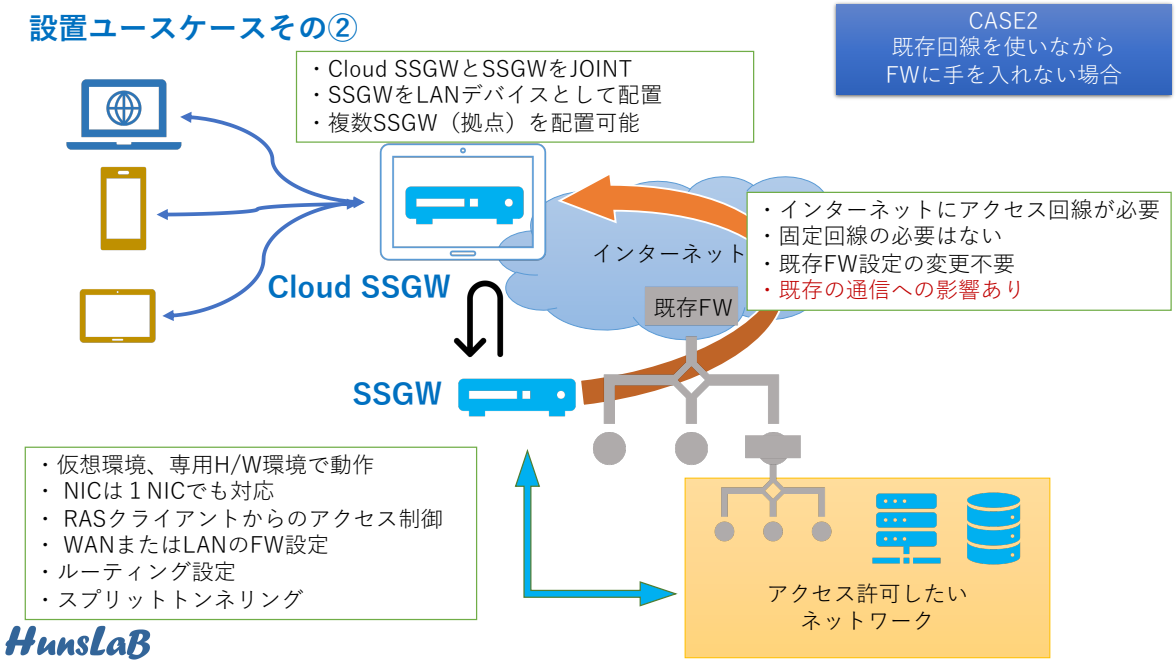
CASE1
既存回線をご利用される場合



HunsLaB

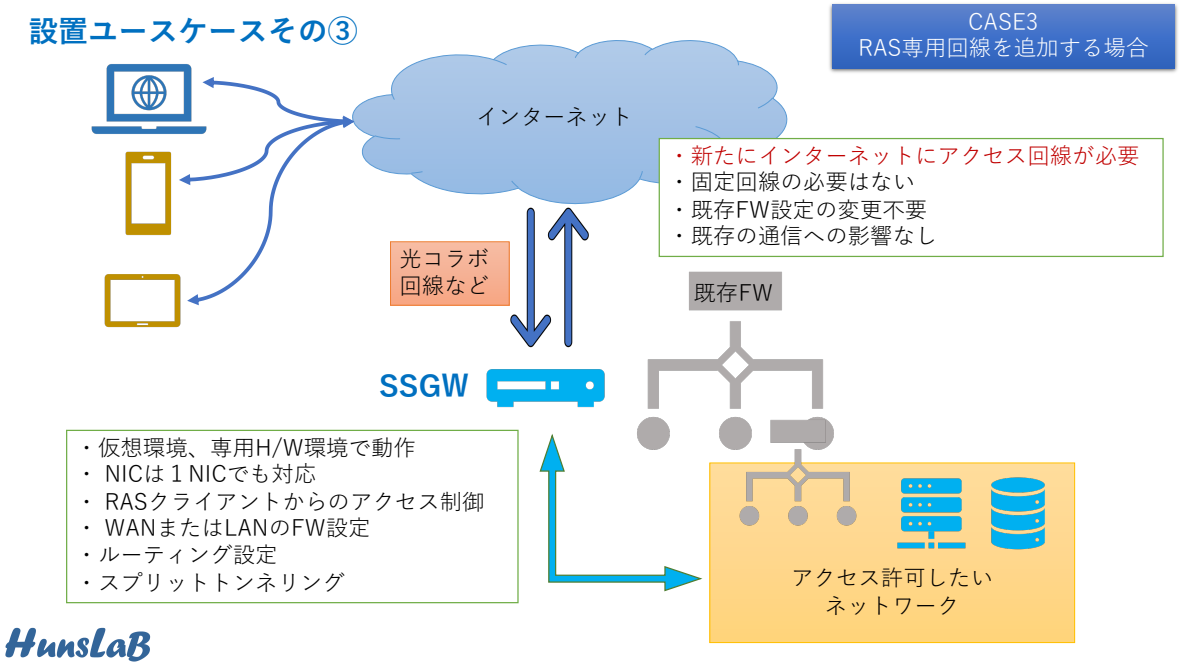
設置ユースケースその②

CASE2
既存回線を使いながら
FWに手を入れない場合

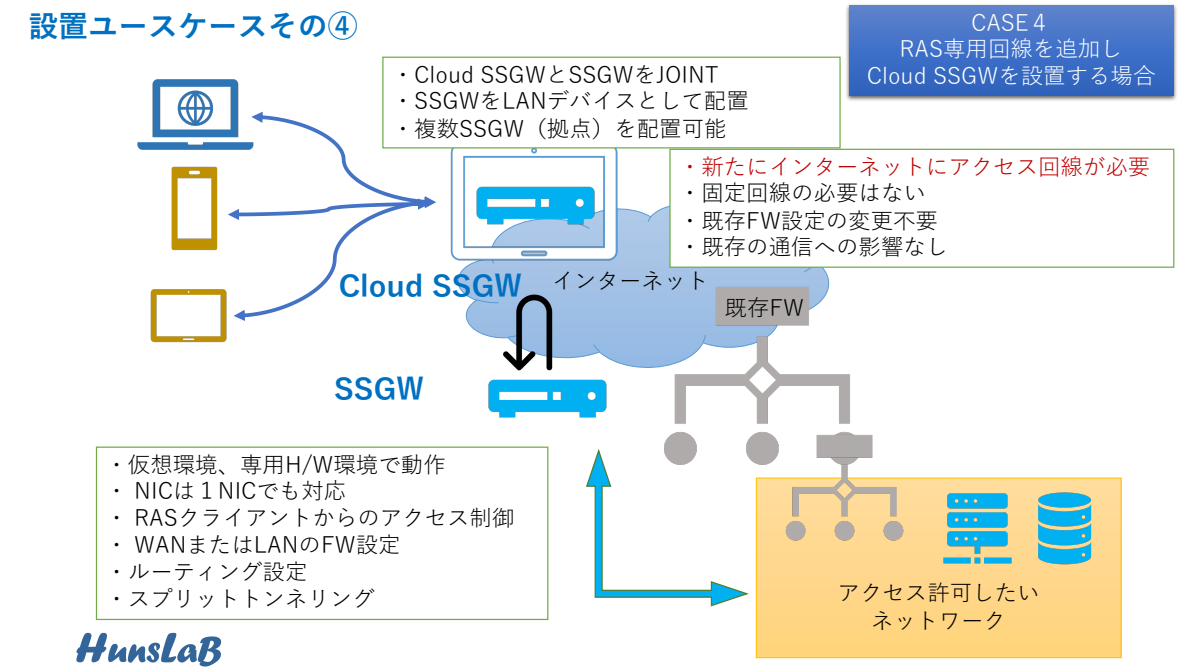


HunsLaB

設置ユースケースその③



設置ユースケースその④



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。