FKEY 安全アクセス

FKEY SConnect

製品説明資料

Windows版 FKEY [エスコネクト]
SConnect
セーフティー リモートアクセスツール

株式会社 応用電子

目次

応用電子

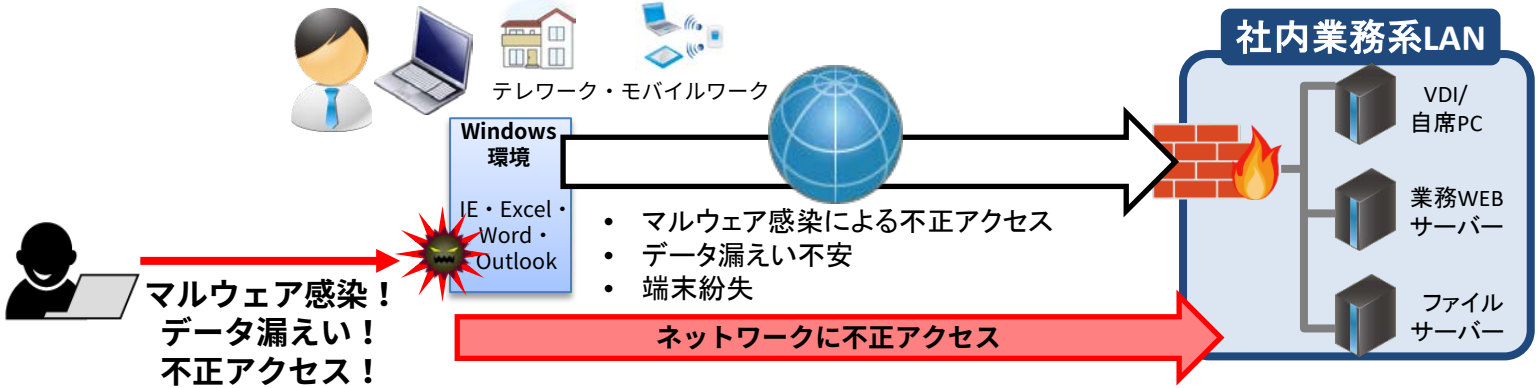
１．製品概要

「FKEY 安全アクセス製品」が解決する問題

応用電子

「働き方改革」
業務効率改善
TCO削減
女性活用
介護離職防止
BYOD
テレワーク推進
BCP対策
パンデミック
自然災害
セキュリティ懸念
顧客データ漏えい
マルウェア被害
端末紛失

モバイルワーク・テレワーク　セキュリティ懸念



FKEY 安全アクセス製品で解決！

応用電子

「安全アクセス技術を応用しワークスタイルの変革をおこす」

FKEY 安全アクセス製品

◎ **FKEY シンクライアント（USBタイプ）**

指紋認証付きUSB型

※ 他に、パスフレーズ認証付きUSB型、microSD型もあります

◎ **FKEY SConnect（ソフトウェアタイプ）**

SConnect Windows ソフトウェア

USBタイプ / ソフトウェアタイプの2種類

- FKEY 安全アクセス製品をPCに導入
- PCが業務系LANアクセス用端末になります

マルウェア感染！
データ漏えい！
不正アクセス！

安全アクセス！

社内業務系LAN

- 社内業務環境に安全にアクセス
- 会社に出社することなく
  いつも通りの業務を遂行

製品① FKEY シンクライアント

応用電子

USBデバイス型

- USBデバイスを挿入して起動するだけでPCが安全アクセス端末に
- PCに導入するエンドポイントソリューション。サーバーやクラウドの導入不要でPCだけで動作。

特徴①
PCに挿入して再起動

特徴②
Windows環境不要
（ディスクレスPCでも可）

特徴③
Windows環境のマルウェア分離

特徴④
業務環境に安全アクセス

Windows環境
IE・Excel・Word・Outlook等

Windowsと分離

セキュア環境
業務環境にアクセス

- PCのWindows不使用
- ディスクアクセス不可
- データ共有不可

安全アクセス！

社内業務系LAN
VDI/自席PC
業務WEBサーバー
ファイルサーバー

ネットワークアクセス

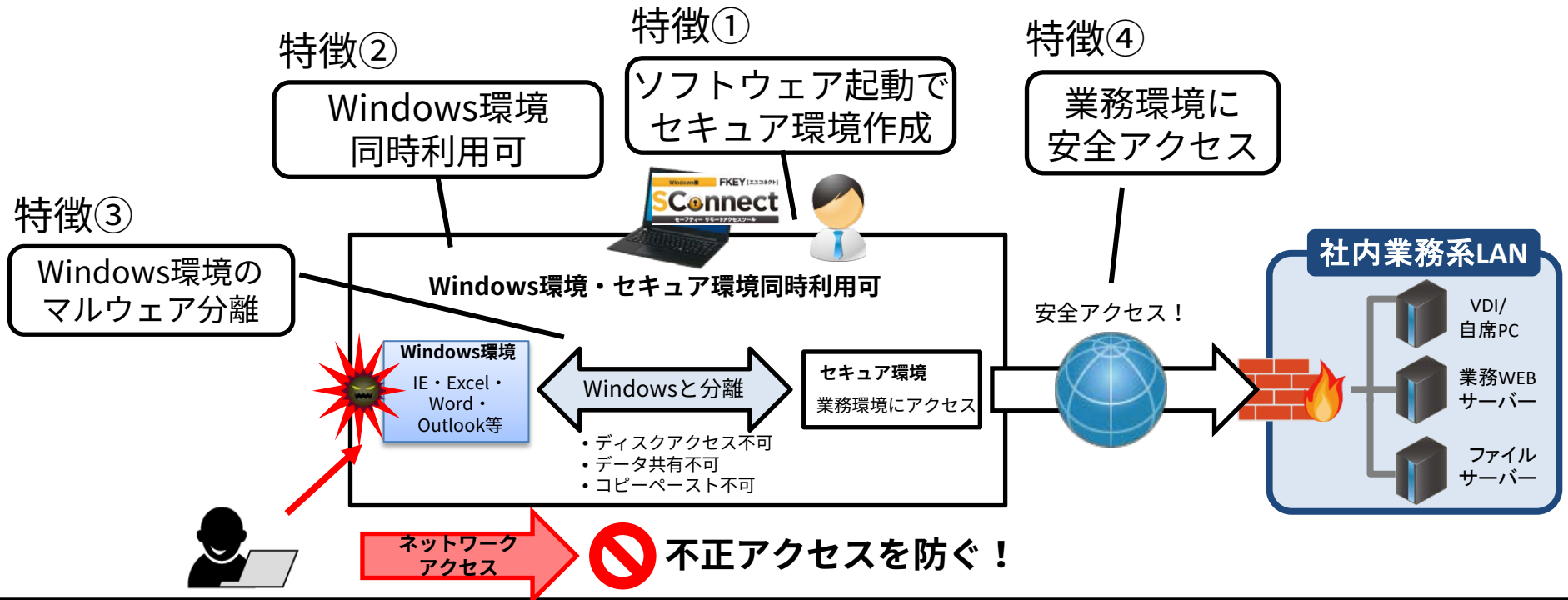
不正アクセスを防ぐ！

製品② FKEY SConnect

応用電子

Windows ソフトウェア
(Windows10 Pro/8.1 Pro)

- FKEY シンクライアントの機能をソフトウェアで実現
- 1台のPCをWindows環境とセキュア環境のハイブリッドな安全アクセス端末に
- PCに導入するエンドポイントソリューション。サーバーやクラウドの導入不要でPCだけで動作。

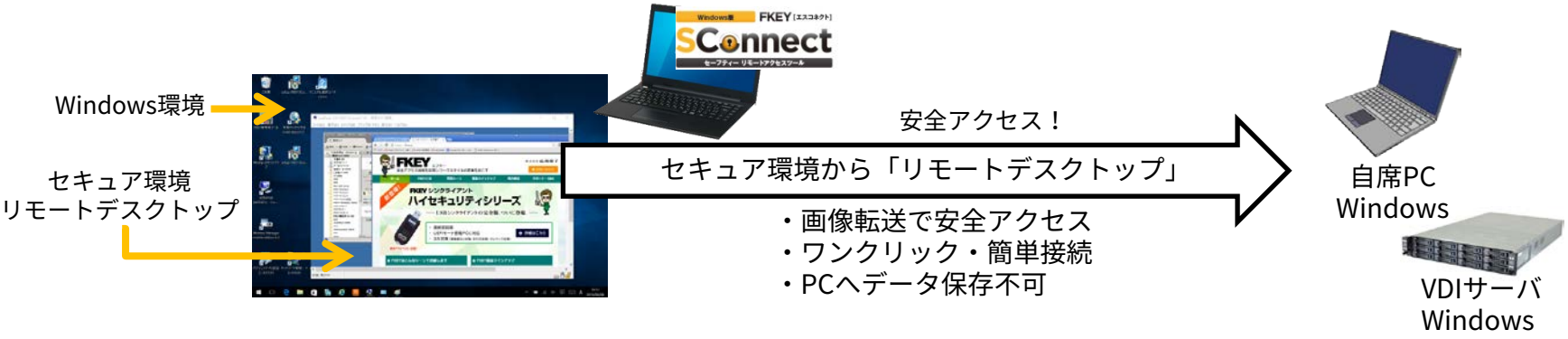


FKEY SConnectによる安全アクセス機能

応用電子

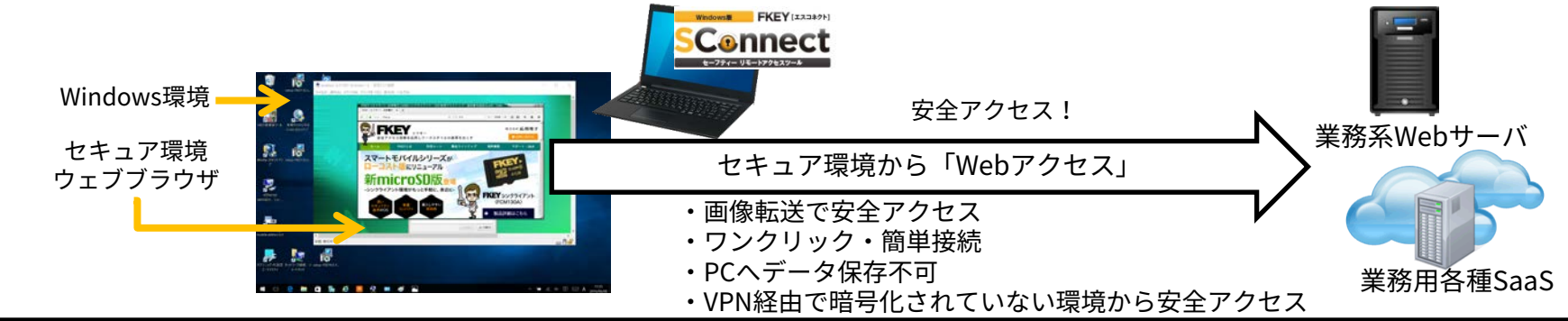
セキュア・デスクトップ機能

PCから業務系LANのデスクトップにアクセス



セキュア・ブラウザ機能

PCから業務系LANのWeb環境にアクセス



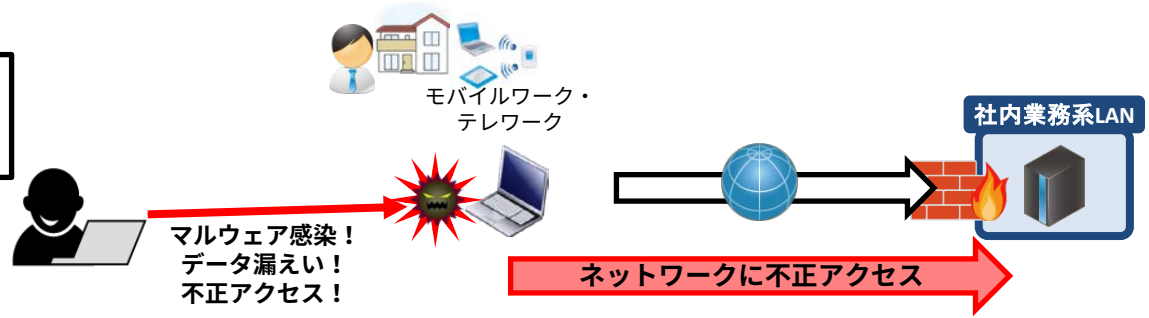
2. 利用シーン

利用シーン① テレワーク・モバイルワークに

応用電子

FKEY導入前

1. モバイル・テレワークで使用するPCがマルウェア感染
2. 感染PCで社内LANにアクセス
3. マルウェアによる遠隔操作で社内LANに侵入
4. データ漏えい・不正アクセス発生



FKEY導入後

1. モバイル・テレワークで使用するPCがマルウェア感染
2. FKEYを起動（ソフトウェア起動またはUSB起動）
3. FKEYのセキュア環境から社内LANにアクセス
4. マルウェアはセキュア環境にアクセスできません
5. 安全に社内LANで業務を遂行

利用シーン② 業務系LANに安全アクセス

応用電子

FKEY導入前

1. 社内PCで情報系LANにアクセスし、マルウェアに感染
2. 感染PCで個人情報を扱う社内業務系LANにアクセス
3. マルウェアによる遠隔操作で社内業務系LANに侵入
4. 個人情報漏えい・書き換え等の不正アクセス発生

問題点

- 端末2台持ちで業務分離
- ネットワークを分離
- 高コスト・低利便性

FKEY導入後

1. 社内PCで情報系LANにアクセスし、マルウェアに感染
2. FKEYを起動（ソフトウェア起動またはUSB起動）
3. FKEYのセキュア環境から個人情報を扱う社内業務系LANにアクセス
4. マルウェアはセキュア環境にアクセスできません
5. 安全に社内LANで業務を遂行

利点

- PC1台でOK。低コスト。
- FKEY安全アクセスを起動して業務LANにアクセス
- 簡単導入。PCにFKEYを導入するのみ。サーバやクラウド不要

利用シーン③ 顧客先対応・業務委託に

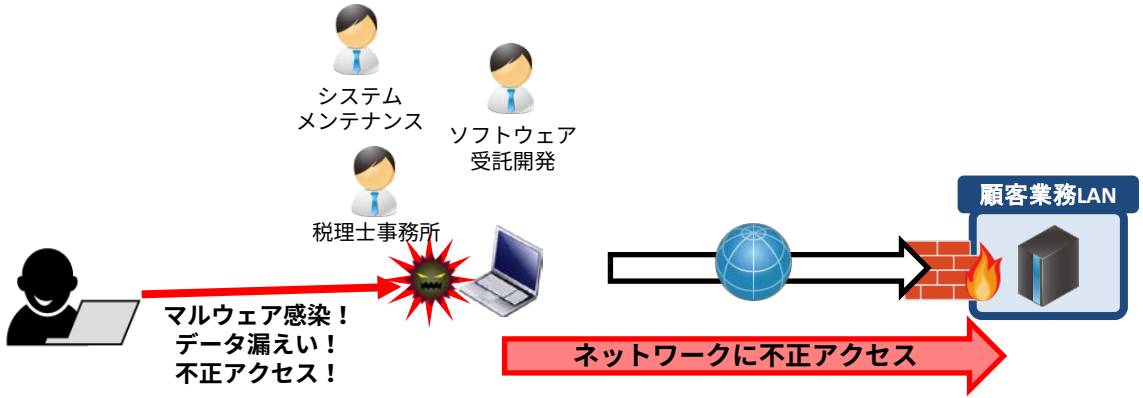
応用電子

FKEY導入前

1. 顧客先のLANにアクセスするPCがマルウェア感染
2. 感染PCで顧客先LANにアクセス
3. マルウェアによる遠隔操作で顧客先LANに侵入
4. データ漏えい・不正アクセス発生

問題点

- 顧客先データ漏えい
- 顧客先での業務遂行が望まれる（業務効率低下）

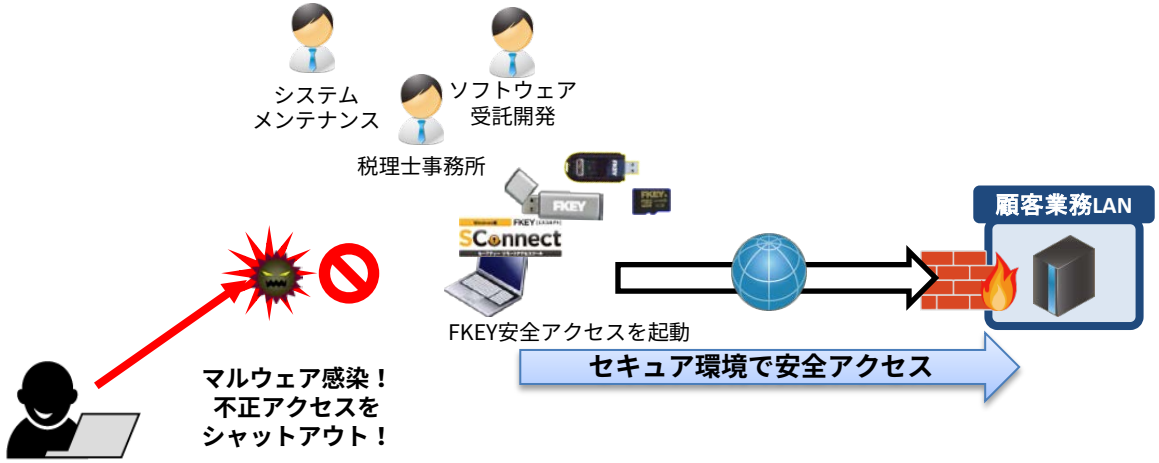


FKEY導入後

1. 顧客先のLANにアクセスするPCがマルウェア感染
2. FKEYを起動（ソフトウェア起動またはUSB起動）
3. FKEYのセキュア環境から顧客先LANにアクセス
4. マルウェアはセキュア環境にアクセスできません
5. 安全に顧客先LANで業務を遂行

利点

- PC1台でOK。低コスト。
- FKEY安全アクセスを起動して顧客業務LANにアクセス
- 簡単導入。PCにFKEYを導入するのみ。サーバやクラウド不要



3．競合製品比較

シンクライアント端末との比較

応用電子

Windows 10 ProとFKEYのハイブリッドで
利便性とセキュリティの両方を満たす

シンクライアント方式	FKEY SConnect	シンクライアント端末（Windows OS）	シンクライアント端末（専用OS）
OS	Windows 10 Pro / 8.1 Pro＋FKEY OS	Windows 10 IoT 等	組込Windows/Linux等
利用可能なアプリケーション	セキュア環境(FKEY OS)： • セキュア・デスクトップ リモートデスクトップ安全アクセス • セキュア・ブラウザ 社内Webシステム安全アクセス Windows環境(Windows 10 Pro / 8.1 Pro)： • 通常のWindowsとして使用可能	Windows環境： • 社内アクセス • リモートデスクトップ • ブラウザ • その他(Windowsの設定による)	リモートデスクトップ環境 • 社内アクセス • リモートデスクトップ
利便性	◎	○	△
	• Windows機能・アプリ利用可 • 端末の選択肢が豊富（市販PC利用可）	• Windows機能・アプリ利用可 • 端末の選択肢が少ない	• リモートデスクトップ専用 • 端末の選択肢が少ない
セキュリティ	◎	△	◎
	• Windows環境がマルウェア感染してもFKEY環境で業務系LANに安全アクセス • FKEY環境からWindows環境へのファイル／テキストコピー・ペース／ディスクアクセス不可 • Windows環境からFKEY環境へのネットワークおよびディスクアクセス不可	• Windows がマルウェア感染し、リモートデスクトップおよびブラウザに影響をおよぼすリスクあり	• Windowsアプリ利用不可のため感染リスクが低い

4. 製品仕様

FKEY SConnect 機能仕様

FKEY SConnect

【機能仕様】

機能	内容
ネットワーク接続機能	PCのハードウェアに依存する
VPN機能	F5 Networks, BIG-IP APM (Network Access) Juniper Networks, Junos Pulse Secure Access (Network Connect) Cisco Systems, ASA 5500-X Series Next-Generation Firewalls (Cisco AnyConnect SSL-VPN, IPsec) L2TP/IPsec, Fortinet, FortiGate (SSL-VPN トンネルモード)
セキュア・デスクトップ機能	Windows Remote Desktop Service (RDP), Citrix XenApp / XenDesktop (ICA) VMware Horizon
セキュア・ブラウザ機能	FKEY分離環境でブラウザを起動して外部や内部Webサイトに安全アクセスする機能
ワンクリック接続・簡単接続機能	事前に設定したWebサイトや仮想デスクトップに簡単に接続ができる機能

FKEY 安全アクセス製品

応用電子

製品名	FKEY SConnect	FKEY シンクライアント
製品形態	Windowsソフトウェア	USBデバイス
利用方法	アプリケーション起動	USB端子挿入・PC再起動
分離セキュリティ方式	ソフトウェア分離	ハードウェア分離
Windows環境	Windows 10 Pro 64bit 日本語版 Windows 8.1 Pro 64bit 日本語版	Windows OSを使用しない （ディスクレスPC可）
必要メモリ	４GB	２GB
Windows利用	セキュア環境と同時使用可能	Windows環境を使用する場合 セキュア環境と同時使用不可
安全アクセス機能	• セキュア・デスクトップ機能 • セキュア・ブラウザ機能	• セキュア・デスクトップ機能
販売方法	サブスクリプション契約 (1年1パック/1年10パック/1年100パック)	買い切り型
価格	Open (1年1パック/1年10パック/1年100パック)	Open
サポート	サブスクリプションに含まれる	別途契約 3,600円/年（指紋版、パスフレーズ版） 1,200円/年（microSD版）

付録A. FKEY SConnectの分離技術について

FKEY SConnectの分離技術 Hyper-VとFKEY OS

応用電子

Hyper-V

- Microsoft社の仮想化技術
- １台のWindowsサーバ上で複数のWindows環境を起動させることが可能になる
- Windows Serverの機能として実装されている
  - Windows Server 2008～

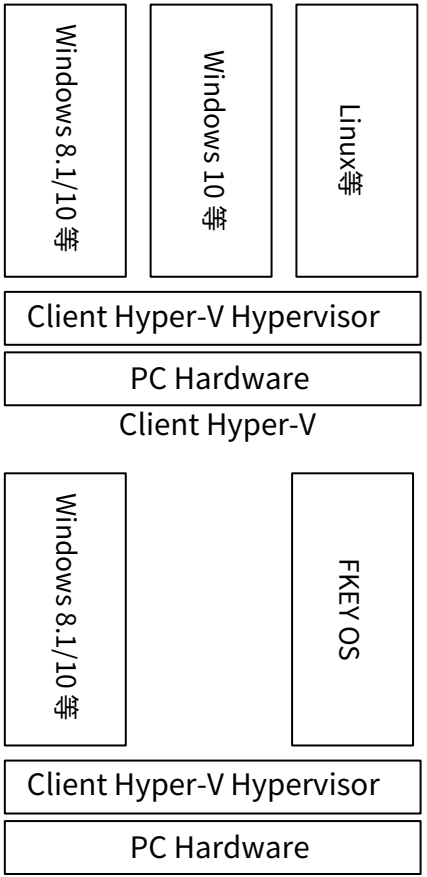
クライアントHyper-V

- Microsoft社の仮想化技術
- Windows サーバで使用可能だったHyper-VをWindows でも使用できるようにしたもの
- １台のWindows PC上で複数のWindows環境を起動することが可能になる
  （Linuxも動作可能。サポートしているOSはMS社のサポートページに記載）

- Windows 8.1 Pro / Windows 10 Pro 64bitの機能として提供されている
  （サポートしているHWのスペック詳細はMS社のサポートページに記載）
- 4GBのRAMで基本的な仮想マシンを3,4台起動することが可能

FKEY SConnect

- Client-Hyper-V の技術を利用
- Client-Hyper-VのゲストOSとしてFKEY OSを動作
- Client-Hyper-VのホストOS（PCのWindows）とゲストOS（FKEY OS）を分離



Client Hyper-Vをよりセキュアに

- **FKEY環境改ざん防止機能**
  FKEYで使用する仮想ハードディスクファイルがユーザによる意図的な操作やWindowsに感染したウイルス等により編集された場合、FKEYは起動不可となります。

- **FKEY環境のデータ暗号化**
  FKEYではNW/VPN/VDI接続情報を管理者ツールで作成し、その後専用のツールを使用して、仮想ハードディスクファイル内へ書込みます。
  書き込まれた接続情報は暗号化されているため、万が一PCの紛失や窃盗が発生した場合でも情報漏えいの可能性は極めて低くなります。

- **Swap領域暗号化**
  FKEY利用中にswapが発生した場合、その情報は仮想ハードディスクファイル内に書き込まれますが、内容は暗号化されています。
  そのため、swap領域のなかに機微情報が含まれていたとしても、仮想ハードディスクファイルを解析してその情報を取り出すことは出来ません。

- **複製不可**
  FKEYは専用アプリのみからの起動制限とライセンス認証の仕組みにより、Hyper-Vマネージャのインポート、エクスポート機能を使い他の端末に複製しても起動不可となります。
  悪意ある第三者がFKEYの起動に必要なパスフレーズとエクスポートしたFKEYを入手した場合でもVPN環境に接続することを防げます。

- **FKEY環境のリフレッシュ（ディスポーザブルOS）**
  FKEYは再起動毎に環境がリフレッシュされるため、仮にウイルス感染した場合でも次回起動時に影響を受けません。

- **FKEY環境に接続可能デバイス制限**
  FKEYではWindowsに接続したハードディスクドライブ(物理、仮想)、USBデバイス、光学ドライブ等を利用する設定を行えないため、それらのデバイス経由でのウイルス感染やユーザによる意図的な機微情報のWindows<->FKEY間の移動を防げます。

- **Windows<->FKEY データ連携制限**
  ファイルのコピー、共有フォルダの利用、クリップボードの共有、ファイルのドラッグ＆ドロップ等の利用を制限しているため、ウィルスやユーザによる意図的な操作、または誤操作による機微情報のWindows<->FKEY間の移動を防げます。

株式会社 応用電子
電話(代表)：03-5888-4015
FKEY製品サイト：https://fkey.jp/