Inuvika ユースケース

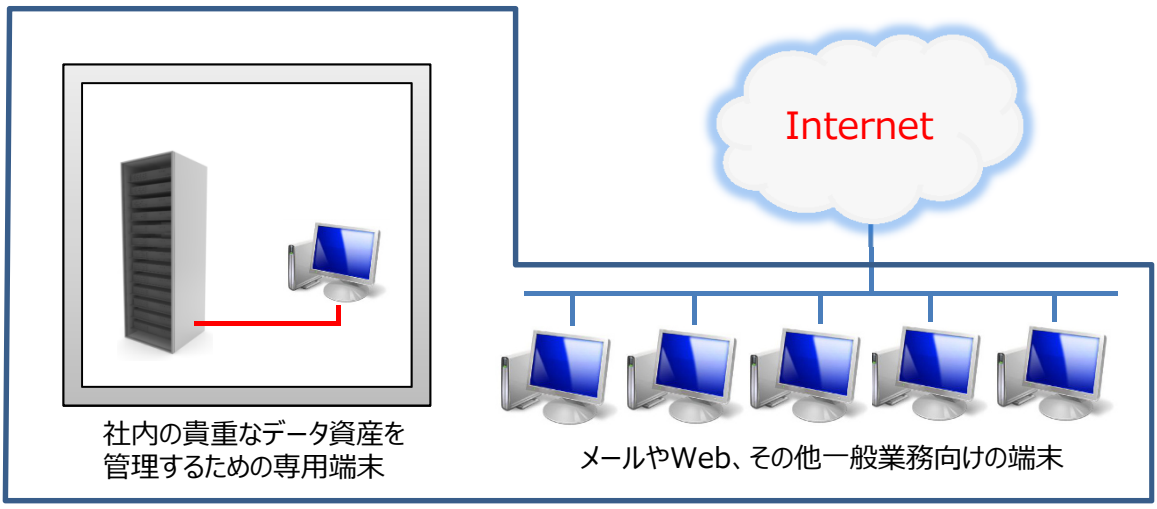
CROSS HEAD

Inuvika Open Virtual Desktop（OVD）Enterpriseで標的型攻撃対策

1. 内部ネットワークを“外部から隔離”することで、貴重なデータ資産を安全に保護します。

- 年金機構などで大きな問題となった『標的型攻撃』。 社内PCがマルウェア（悪意のあるソフトウェア）に感染し、遠隔操作により機密情報を詐取される事象が多発しています。アンチウィルスソフトや、UTM（統合脅威管理）アプライアンスの登場により、セキュリティは向上していますが、必ずしもゼロデイ攻撃（まだ認知されていない未知の攻撃）を完全に防ぐことは現状では困難です。

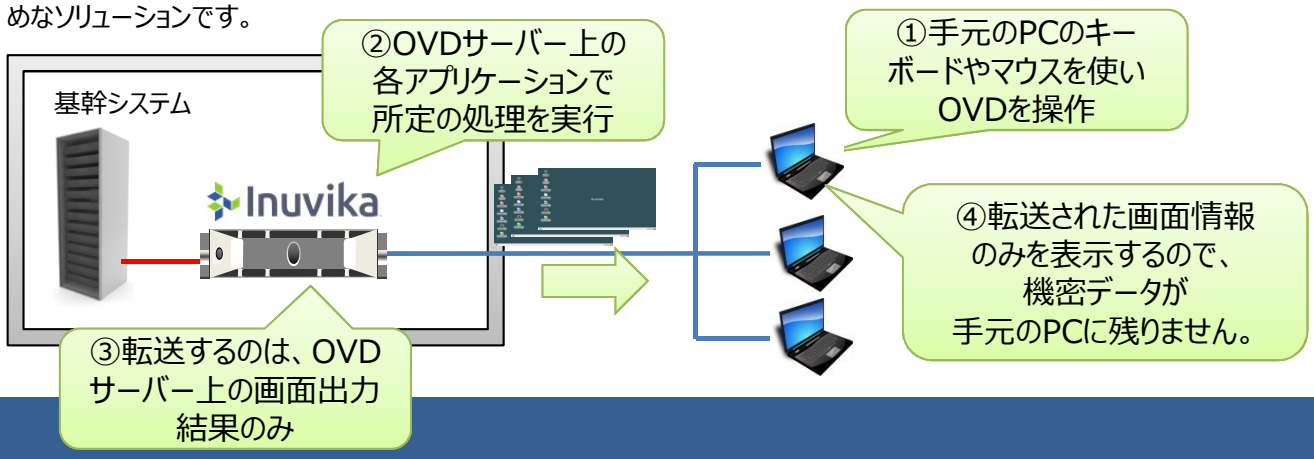
- 究極のセキュリティとは、社内の貴重なデータ資産をネットワークから分離することです。閲覧を行うための 専用の端末を用意することで、インターネットからの侵入を防ぐことができます。



- 上図の場合、情報流出事故は確実に低減することができます。しかし、データ資産を閲覧するたびに専用端末へ移動しなければならないのは、利用者にとって非常に不便であるだけでなく、極めて非効率であると言わざるを得ません。そこでデータ資産を保護しつつ、かつユーザーの利便性を確保するといったことで、今注目を集めているのが、Inuvika Open Virtual Desktop（OVD）Enterpriseです。

2. Inuvika Open Virtual Desktop（OVD）Enterpriseとは？

- OVDは、ユーザがOVDサーバーを経由して基幹システムのファイルにリモートアクセスを行い、その画面出力結果だけを手元のPCに映し出すクライアント仮想化ソフトウェアです。その為、手元のPCには、OVDを経由してアクセスした機密データが何も残りません。セキュリティを確保しつつ利用者の利便性を両立したい、セキュリティ意識の高いお客様にお勧めなソリューションです。

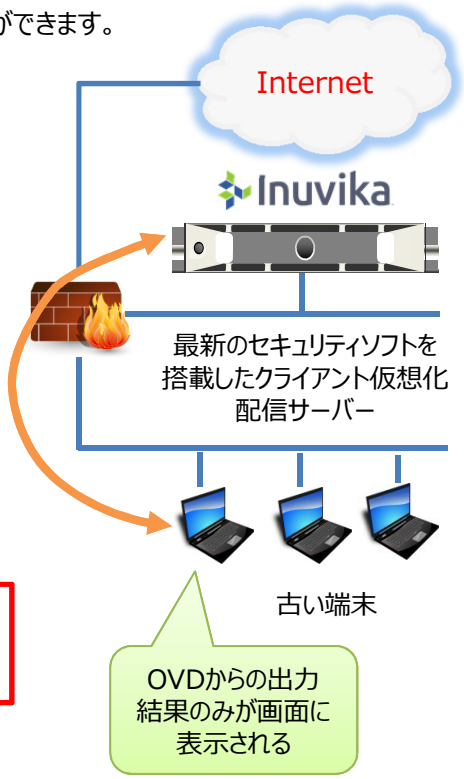


3. OVDで標的型攻撃対策と利便性の両立が可能に

- 手元の端末に機密データが残らない為、外出先でも安全にファイルの閲覧ができます。
- 古い端末でも、インターネットに安全にアクセスすることが可能です！

  右図のように、OVDサーバーと古い端末間のやり取りは、キーボードやマウスの入力結果と、その実行結果を出力した画面のみです。古い端末自体が、インターネットに直接アクセスすることがないため、セキュリティを保つことができます。またOVDサーバーは常に最新のセキュリティを維持することで、リスクを最小限に保ち、万一マルウェアに感染しても、FWにてマルウェアからの通信をブロックすることで、LANセグメントを隔離します。
- 手元の端末で機器故障が発生しても、すぐに自分の環境を利用することが可能です。

  利用者は遠隔のOVDを操作しているため、設定変更などの情報は手元の端末に残りません。その為、端末が故障して交換しても、遠隔のOVD上のユーザー設定を継続利用でき、再設定の手間を省きます。



クライアント仮想化配信サーバーを利用することで、セキュリティと利便性の向上をもたらします。

4. OVDの様々な特徴と機能、そして高いコストパフォーマンスで、お客様のビジネスをサポート

スモールスタートを可能にする、オールインワンな、サブスクリプションライセンス。

追加費用なしで、サポートと最新のアプリケーションをご提供。

iPad/Androidタブレット、スマートフォン、PCなど様々な端末で利用可能。

Linux/Windowsアプリケーションの同時配信が可能。
Linuxシステムだけを利用すれば、Windows用の各種ライセンスの購入は不要です。

標的型攻撃対策や、BYOD・リモートオフィスを簡単に実現できる価格体系です。

お問い合わせ・お見積りは
クロス・ヘッド株式会社
ソリューション事業部　ソリューション営業部

〒１５０－６０２７
東京都渋谷区恵比寿４-２０-３ 恵比寿ガーデンプレイスタワー27Ｆ
TEL:03-5793-3381
URL:http://www.crosshead.co.jp/products/virtual/
Mail: ch-solution@crosshead.co.jp