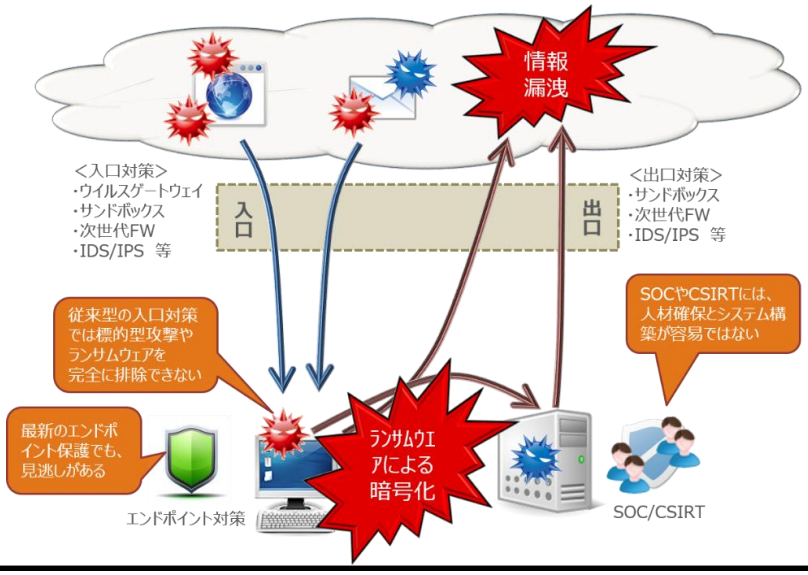
S&J Secure VDI （クラウドサービス）

本サービスご提供の背景

標的型攻撃やランサムウェアなどマルウェアによる脅威は増大しており、被害も拡大しています。そのため、「感染を前提」とした対策では、サンドボックスやSIEMを実装したSOCやCSIRTの体制構築などの高度なセキュリティ対策が求められています。

一方で、高度なセキュリティ対策を続けてきた大きな組織では、未知のマルウェアの検知や監視によるソリューショ ンでは対策としては限界があり、根本的な対策へのニーズが高まっています。

もう一方で、サンドボックスやSIEMを用いた高度なセキュリティ対策は非常にコストが高いため、実装できない組織が大半となっています。



本サービスのコンセプト

従来の入口/出口/内部対策には限界があることから、仮想化技術を用いた無害化というコンセプトでのセキュリティ対策が注目されています。
VDIを用いたソリューションは、Webアクセスによるマルウェア感染やコールバック(C&Cサーバへの情報流出)に対して大きな効果が期待できますが、ライセンス費用や複雑なシステム構成による導入コストが課題です。

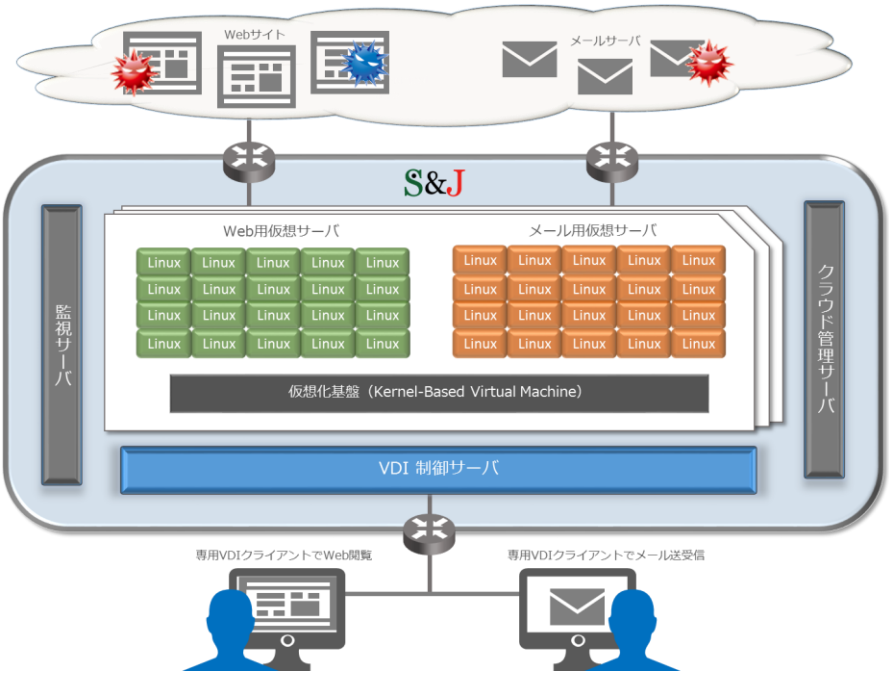
S&Jは、オープンソースをベースとした「S&J Secure VDI」 (以下Secure VDI)を開発し、クラウド上でサービスの提供を開始しました。これにより、導入/運用コストの大幅な削減と導入にかかる期間を大幅に短縮することができるようになりました。

Secure VDIを利用することにより、標的型攻撃やランサムウェアにおける従来の「感染を前提」とした入口対策、出口対策に比べて、飛躍的にセキュリティレベルを向上させることができます。 主な特徴は以下となります。

- ・クラウドサービス（日本国内データセンター）
- ・利用者単位の専有ゲストOS
- ・ゲストOSはLinux
- ・ゲストOSは毎回リフレッシュ
- ・Web、メールに対応
- ・ファイル受け渡し

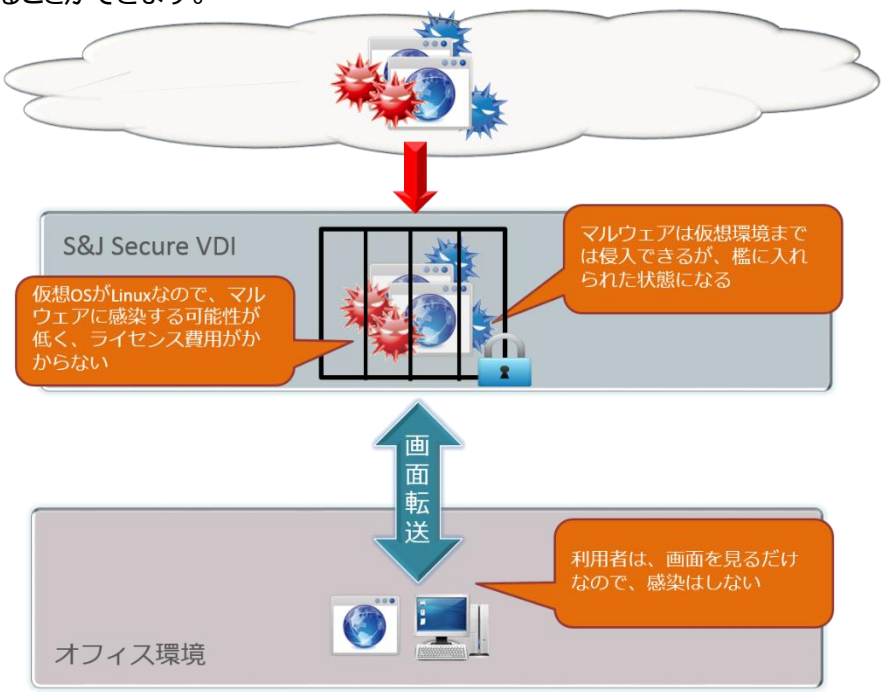
S&J Secure VDIの構成イメージ

Secure VDIでは、主な感染原因や情報漏えいの原因となる「Web利用」と、「メール利用」を分離するための仮想環境をご提供し、Webやメールで重要な情報を保有している端末が感染しない環境、コールバックが発生しない環境（お客様側のインターネットの出口制限は別途必須）をご提供致します。



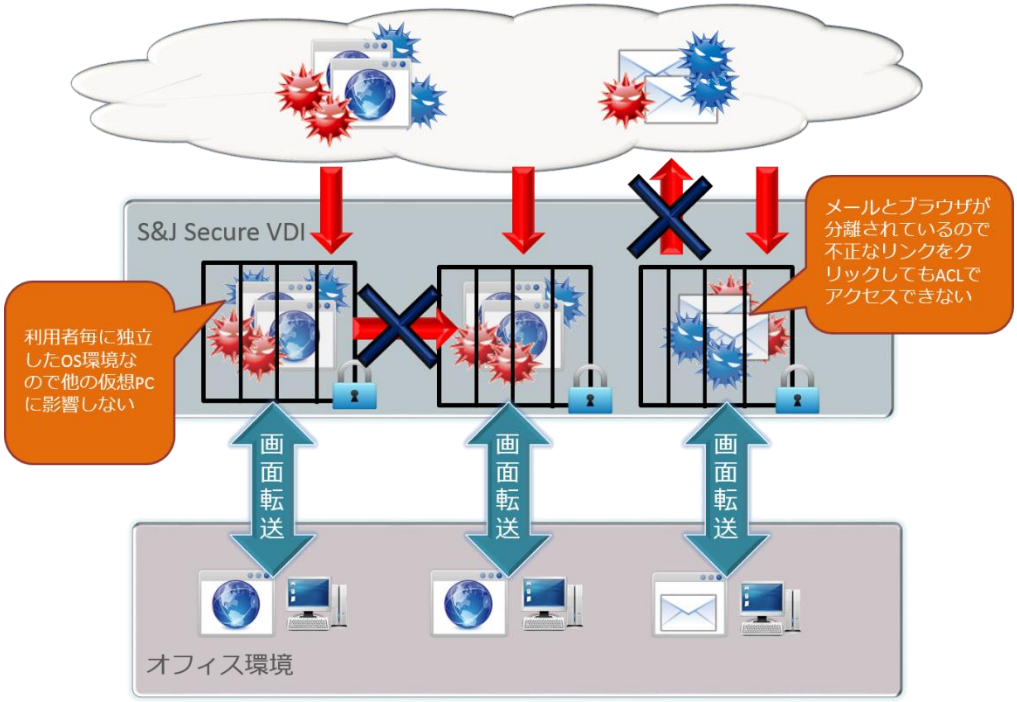
特徴①　仮想環境と画面転送による無害化

仮想PCでブラウザやメールを利用し、利用者はその画面を見るだけなので、利用者のPCそのものはマルウェアは感染しません。また、仮想PCのOSはLinuxなので、マルウェアに感染する可能性が極めて低く、また、コストを大幅に削減することができます。



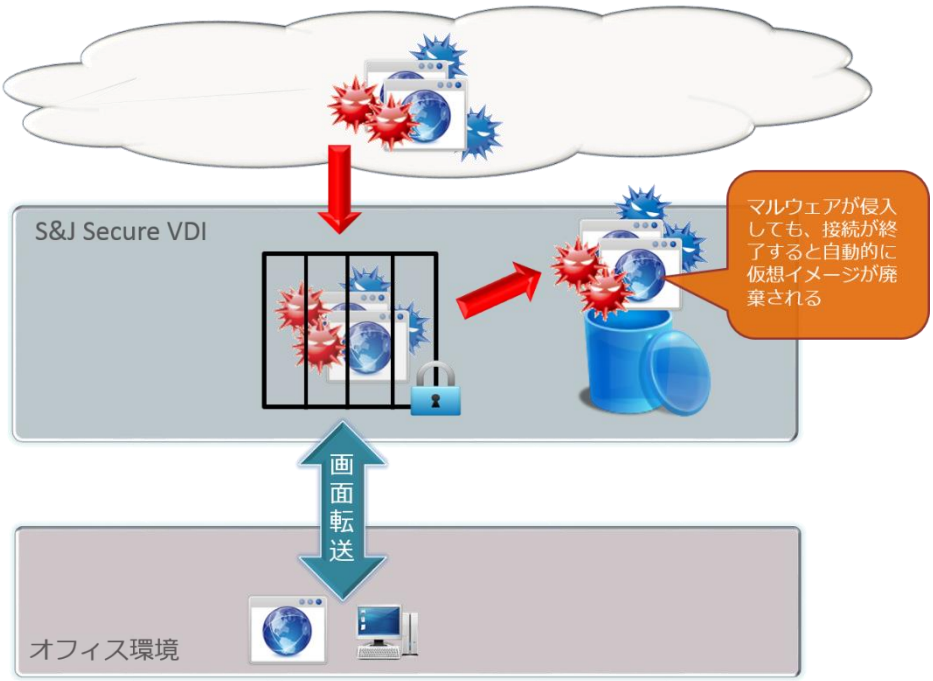
特徴②　利用者毎、利用サービス毎に独立した仮想環境

仮想PCは、OS単位でサービス(Webブラウザ、メール)ごとに利用者が専有します。仮想PC間のアクセスは禁止されており、メール利用仮想PCからはWebアクセスはできませんので安心です。



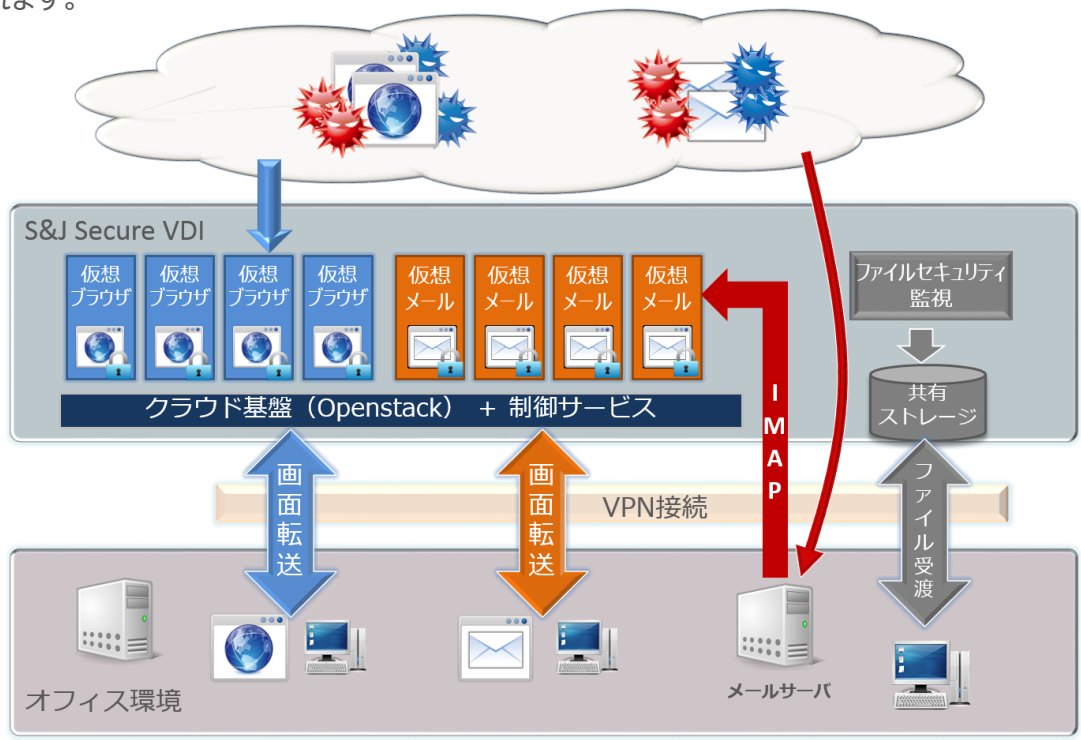
特徴③　利用するたびにリフレッシュされる

利用者が利用を終了すると、自動的に仮想イメージが削除され、再び利用するときにはフレッシュな仮想PCになりますので、マルウェアが潜む心配はありません。



特徴④　Webブラウザ,メールに対応し、ファイルの受け渡しも安全にできる

Webブラウザ、メール利用に対応しており、それぞれファイルの受け渡しができます。ファイルはサンドボックスで検査されます。

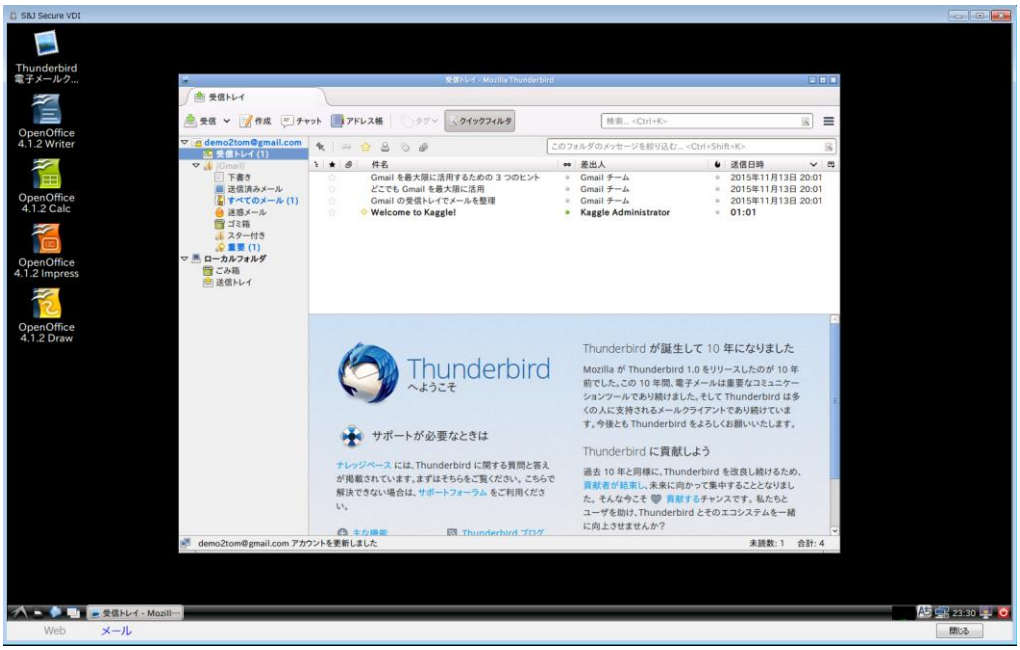


Webブラウザの利用画面イメージ

専用アプリを使って、Webブラウザを利用します。

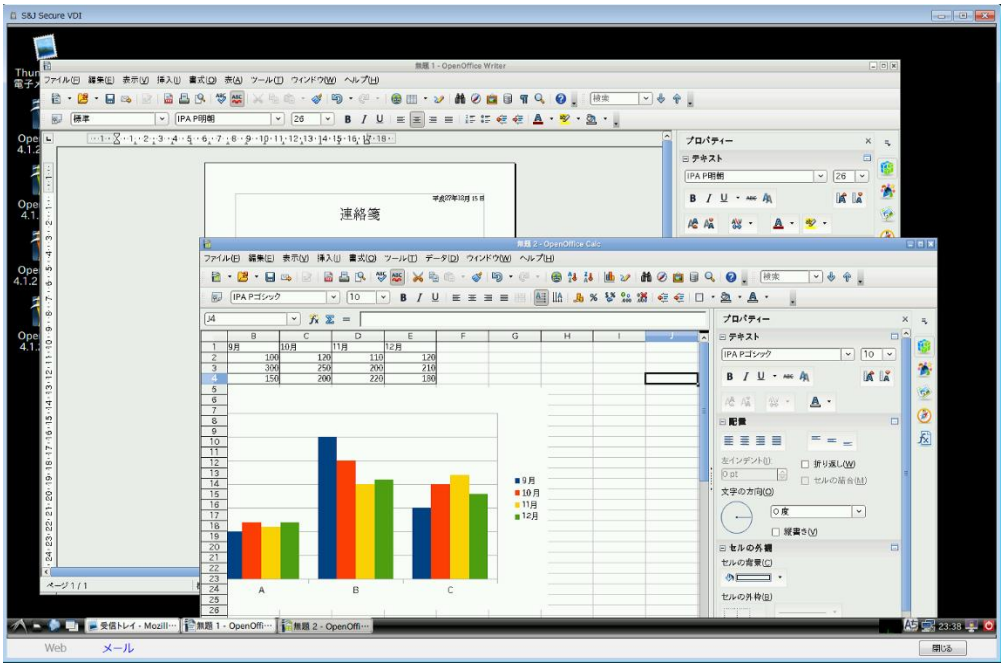
メールの利用画面イメージ

専用アプリを使って、メールを利用します。



オフィスアプリケーションの利用イメージ

Linuxで動作するオフィス互換アプリケーションで、オフィスファイルを開くことができます。



≪お問合せ先≫
株式会社シーアイエー（ 092-432-4877 / info@c-i-associates.co.jp ）
CIA Cyber Integrated Associates