

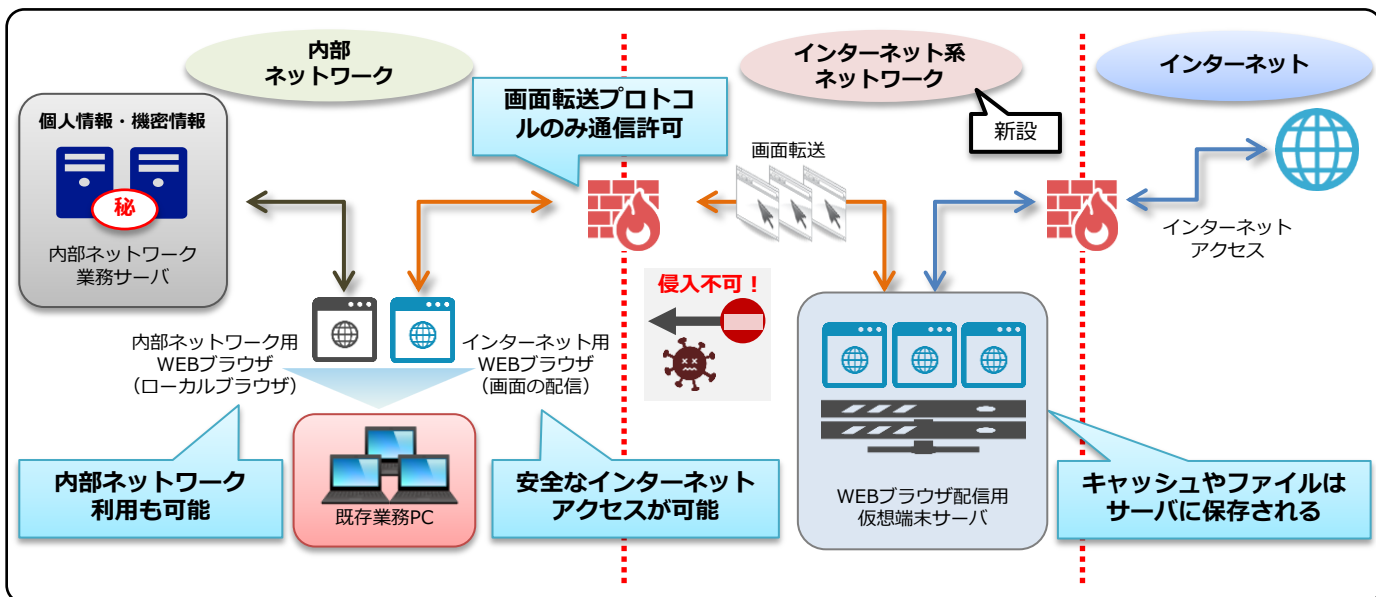
アライドテレシスの 情報セキュリティ強靱化ソリューション

情報セキュリティ強靱化ソリューションのポイント

- ✓ インターネット環境を分離することにより、**セキュア**な内部ネットワーク環境を実現
- ✓ ファイル無害化ソリューションにより、ダウンロードファイルの**無害化**を実現
- ✓ メール無害化ソリューションにより、**標的型攻撃への対応**を実現

ソリューション1 「インターネット分離」

- インターネット系ネットワークを新設・分離し、インターネットアクセス用の **仮想端末のWEBブラウザ画面を業務PCへ配信**します。
- 内部ネットワークとの通信は、WEBブラウザの画面転送プロトコルのみを許可しますので、万が一仮想端末がウィルスに感染しても、**内部ネットワークへ侵入することはありません**。
- 内部ネットワークの業務サーバへの接続は通常のWEBブラウザ、インターネットへの接続は仮想端末上のWEBブラウザと使い分けをすることで、業務PC 1台で**安全なインターネットアクセス**を行うことが可能となります。

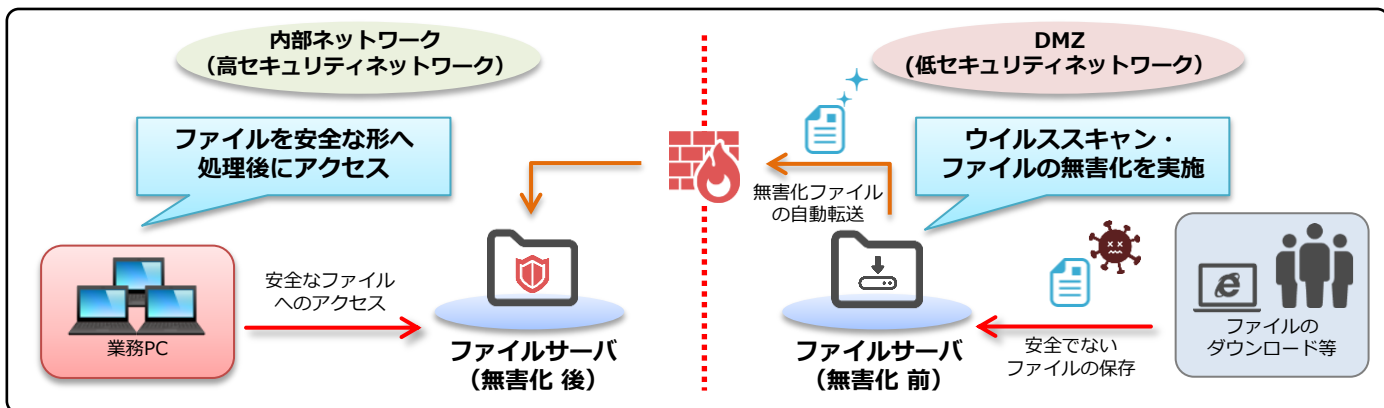


ユースケース：

- ☆ 業務PC から安全にインターネット接続を行いたい。
- ☆ 運用コスト面、利便性の面から、インターネット接続用の専用PC を導入したくない。
- ☆ インターネット分離に興味はあるが、VDIシステムの導入はコスト面・管理面で敷居が高すぎる。

ソリューション2 「ファイル無害化」

- 異なるネットワーク間で、**安全な形でファイルの受け渡しを行う**ことが可能です。
- ファイルサーバに保存されるファイルには、**ウイルススキャンや無害化処理が実行**されます。
- 無害化されたファイルは、**内部ネットワークから安全にアクセス**が可能です。

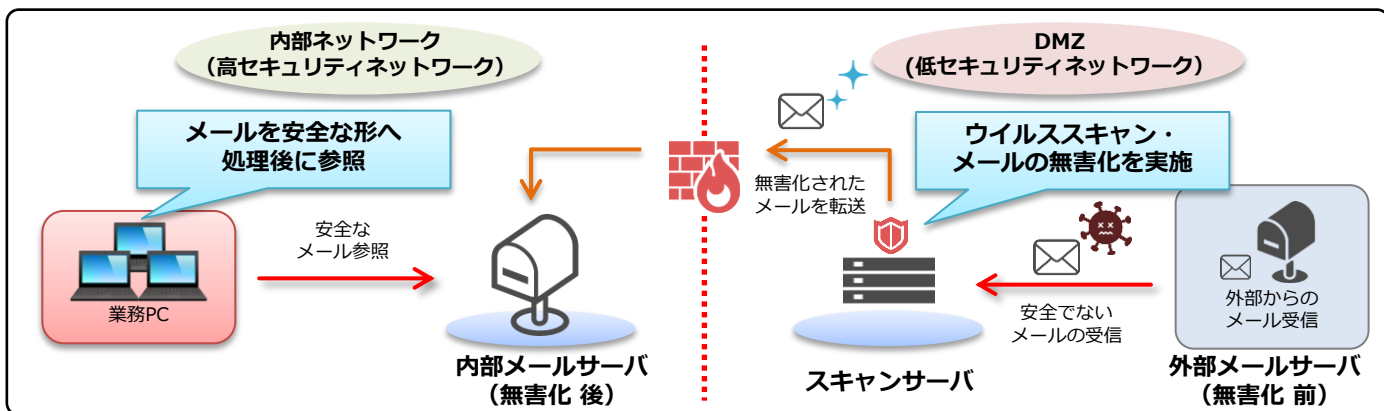


ユースケース：

- ☆ 外部から持ち込んだファイルは、無害化を行ってから業務PCに保存したい。
- ☆ インターネット分離と合わせて、WEBからダウンロードしたファイルを内部ネットワークに安全に保存したい。

ソリューション3 「メール無害化」

- 受信したメールのスキャンや無害化を行い、**安全なメール参照**を可能にします。
- HTMLメールのテキスト化や特定種類の添付ファイルの削除等、**ルールにマッチしたメールを自動で処理**できます。



ユースケース：

- ☆ 標的型メール対策として、攻撃の疑いのあるメールを事前に検知・遮断したい。
- ☆ 情報セキュリティポリシーに沿った形での柔軟なメール制御を設定したい。
- ☆ メール送信時にも、宛先や添付ファイルについての詳細ポリシーを作成したい。

全てのソリューションを組み合わせることも可能です！