

インフォセンス

「水飲み場型攻撃」から重要な情報を守る！ インターネット分離を低コストで実現する「ダブルブラウザ・ソリューション」

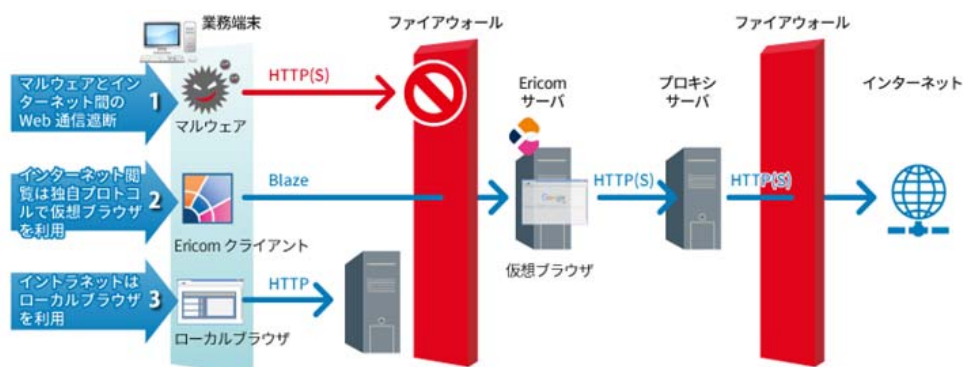
近年、企業や組織・団体が所有している業務端末を標的に、機密情報や個人情報などの重要な情報が漏えいする事故が増加し社会問題となっています。

原因の大半は「標的型攻撃」と呼ばれるもので、フィッシングメールやWebサイト閲覧によるマルウェア感染です。標的型攻撃については年々仕掛けが巧妙になってきており、特に最近では「水飲み場型攻撃」という手法による被害が急増してきています。

「水飲み場型攻撃」とは、特定の組織や個人を狙う標的型攻撃の一つで、標的となる企業や組織・団体がよく利用すると思われるWebサイトを改ざんし、アクセスした利用者にウイルスなどのマルウェアを導入するよう仕込む手法です。サバンナなどで肉食獣が池の周囲などで待ち伏せし、水を飲みた現れた草食獣を狙い撃ちにする様子になぞらえてこのような名称で呼ばれています。

では、「水飲み場型攻撃」に対してどのように対処すれば良いのでしょうか？ 2016年6月以降、総務省を始めIPA・NISCなど各種団体からは業務端末をインターネット環境から分離する対策を行うよう推奨してきており、自治体始め各方面で取組が広がってきています。

インフォセンスでは「水飲み場型攻撃」などの標的型攻撃対策として、お客様へ低コストで導入可能な「ダブルブラウザ・ソリューション」の御提案を行っております。本ソリューションは、仮想化技術を用いて業務端末からインターネットアクセス環境を分離。外部と直接的なインターネットアクセス通信を遮断し「水飲み場型攻撃」を無効化できます。



「ダブルブラウザ・ソリューション」運用イメージ図

「ダブルブラウザ・ソリューション」について

「ダブルブラウザ・ソリューション」はインターネット環境分離のニーズに対して、クライアント仮想化の画面転送の仕組みにより、仮想環境上に用意したブラウザから安全にインターネットを利用させる、セキュリティ強化とユーザの利便性の両立を可能にするソリューションです。

詳細はこちら www.info-sense.co.jp/service/dblbrowser.html

インフォセンスについて

企業価値を高めるITソリューションパートナーであるインフォセンス。その特徴は、企業が保有するモノ<物的資源>のマネジメントに着目したアプローチにあります。

なぜインフォセンスはモノのマネジメントに着目するのか。それは、モノの合理化や効率化、最適化こそ、企業価値を高める要諦だと確信しているから。そして、ITによるモノのマネジメントに誰よりも精通している自負があるからです。

「基幹」「ロジスティクス」「インフラ」のトリプルフォーカスから生まれるITソリューションによって、インフォセンスはお客様の企業価値を高めます。

詳細はこちら www.info-sense.co.jp

《 本件に関するお問い合わせ 》

インフォセンス 営業統括室 営業企画部

担当：高木

TEL：03-3536-3439, FAX：03-3536-3486, MAIL：sales@info-sense.co.jp