安心・安全な商用システムの提供

商用システムのセキュリティを確保

昨今、インターネットを介した不正アクセスや、標的型攻撃と呼ばれるマルウェアによる内部侵入など、情報システムへのサイバー攻撃が激しさを増しています。これらの攻撃に対処するには、最新情報に基づき、情報システムの既知の脆弱性(セキュリティ上の不備)への対処をもれなく行うとともに、攻撃手口を見据えた検知策、被害抑止策の準備が重要となります。また一方、換金性の高い情報や大量個人情報等の不正な持ち出し等の内部不正事件も発生しており、これら重要情報に関わる運用管理の徹底も強く求められます。

NTTデータグループでは、お客様向けに構築、運用する商用システムにおけるサイバー攻撃への対応力強化と内部不正防止の徹底を図るため、①開発段階から適切なセキュリティ対策の作りこみ、②運用中システムの定期的な脆弱性チェック(セキュリティ診断)の定着、③重大な脆弱性発見時の迅速な対応体制の構築、④重要情報に関わる運用管理の徹底、の4つを推進しています。

最新のセキュリティ技術動向に対応

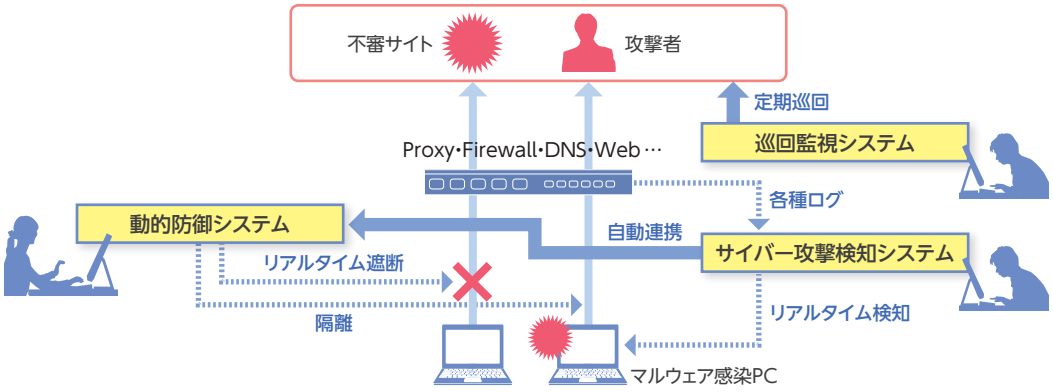
NTTデータグループでは、この推進に当たり、最新のセキュリティ技術動向、脆弱性情報を迅速に共有するとともに、商用システムの開発、運用のプロセスに上記の対応を組み込み、常に安心・安全にご利用いただけるシステムをご提供できるよう取り組んでいます。

情報セキュリティシステム基盤

リスク低減のための社内IT基盤

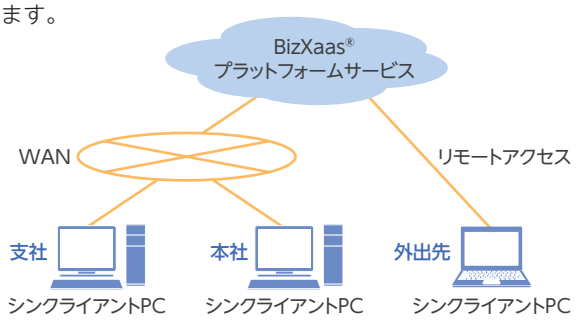
NTTデータでは、社内業務システムのリスク分析を継続的に実施し、新たな脅威による情報セキュリティリスクに対してセキュリティ対策を積極的に社内IT基盤へ導入しています。現在、それらセキュリティ対策の要となるのが「巡回監視システム」「サイバー攻撃検知システム」「動的防御システム」を軸とする、NTTデータが開発・運用する未知マルウェア対策システムです。

巡回監視システムは、定期的にWebサイトを巡回してWebページの改ざんを早期に検知します。サイバー攻撃検知システムは、ネットワーク機器・セキュリティ機器のログをリアルタイムにデータベースへ取り込み、独自に開発した検知パターンを使ってサイバー攻撃を検知し、マルウェア感染PCを特定します。動的防御システムは、サイバー攻撃検知システムからの情報をもとに、PCから不審サイトへの通信を遮断したり、マルウェア感染PCを隔離します。



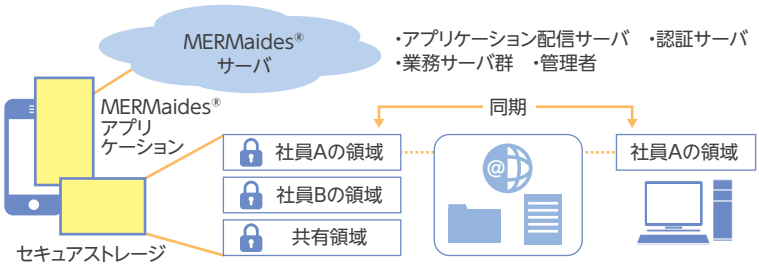
シンクライアント「BizXaaS® Office」DaaS

社員のPC環境をクラウドで提供するサービスが「BizXaaS® Office」です。クライアント環境をクラウド上に集約し、PCをシンクライアントPCに置き換えることでPC側からの情報漏えいを防ぎ、さらにオフィスの省電力化も図っています。また、テレワークを推進するソリューションとして、社内向けにもデスクトップサービスの運用を行っています。



モバイル活用基盤「MERMaides®（マームエイデス）」

モバイル端末内に安全なビジネス領域を確保し、そこに格納された業務アプリケーションやデータを暗号化することで、情報を強固に保護します。モバイルゲートウェイ機能により既存の認証システムと連携し、社内のメールや業務システムとシームレスに同期を取ることで、いつでもどこでも業務を遂行することを可能にします。



NOSiDE®検疫システム

インターネットからの脆弱性を狙ったサイバー攻撃やマルウェアによるインターネットへの情報漏えいを防止する、インターネットアクセス端末を検疫するシステムです。セキュリティ上問題のないPCからの社外サイトへのアクセスはNOSiDE®検疫システムを通して行われます。また、セキュリティ上問題のあるPCを検知するとNOSiDE®検疫システムがアクセスをブロックします。

情報流通インフラ「ETRANPOT」

NTTデータ・NTTデータグループ会社と関連するお客様の間で、セキュアにファイルを転送するシステムです。決められた期間以上は保管できず、また社外からのファイル転送は社内から招待した相手のみ可能となっています。