ソリューション概要

◎現状分析・対策立案コンサルティング

サイバーセキュリティ強化点検サービス	お客様のサイバーセキュリティの対策状況を可視化し、今後実施すべき対策とその優先度を明らかにすることで、最適なサイバーセキュリティ対策計画の策定を支援します。最短2カ月での実施が可能という迅速性に加え、既知の脅威だけでなく、新たな脅威への対策状況も可視化し、常に最新かつ最上のセキュリティレベルの確立を支援します。実際に発生したセキュリティインシデントから得られたノウハウに基づく対策状況のチェックも、NTTデータのサービスならではのものです。
標的型攻撃耐性強化サービス	標的型攻撃を模擬した訓練と、訓練を通じた現状把握と社員への教育を繰り返すことで、攻撃者の侵入を許してしまう確率を減らします。これに加え、一定の割合で攻撃が成功してしまうケースも想定して、どのように内部情報の流出を防ぐかといった「出口対策」の検討も支援します。情報窃取を阻止する観点でのシステムのチェックや、チェックの結果から、さらに耐性を強化する各種ソリューションやサービスの提案へとつなげることができるのも、NTTデータのサービスの特長です。
PCI DSSトータルサービス	日本国内初のQSA(PCI SSC認定審査機関)として、PCI DSS準拠支援コンサルティングをベースに、お客様のシステムに適した世界基準のセキュリティを提供します。計画段階から審査前の最終確認までをトータルサポートする中で、ギャップ分析やシステムのテストで洗い出された課題を解決する各種ソリューションを提供します。審査・報告では、QSAとして訪問調査を実施。認証取得後も、日々の準拠状況を確認し、問題の早期発見と解決をサポートし続けていきます。

◎セキュリティ対策ツール導入・運用

多要素認証技術「BXA(BizXaaS-Authentication)」	ユーザの手元にトークンがある場合に限り認証するという、強固で確実な本人認証を提供します。仮にWeb上でパスワードを盗み取られても、そのパスワードは1分後には二度と使用できなくなり、なりすましによるログインを防ぎます。近年脅威が叫ばれているマルウェアによる不正送金攻撃にも対応しており、ログイン後のマルウェア攻撃に対応した新型のワンタイムパスワードを提供することも可能です。これまで国内金融機関80社以上、法人企業30社以上という圧倒的な導入実績を誇っています。

統合ID管理「VANADIS® Identity Manager」	純国産ソフトウェアなので、兼務情報や組織構造など日本独自の商習慣をきめ細かくサポートした統合ID管理を実現します。プロビジョニング機能やグループ管理機能、シングルサインオン機能など、豊富な機能をそろえているため、お客様それぞれの組織事情に適合した運用が可能です。様々なシステムと連携するインターフェースを搭載するとともに、確立したフレームワークにより短期間で構築できるのも特長です。NTTデータの自社使用ソフトウェアをベースとしており、10年以上の運用実績による信頼性を誇ります。
ネットワークセキュリティ診断サービス	ネットワーク機器やサーバ等のお客様のネットワークシステムを多様な手法で検査し、セキュリティの問題点がないかを明確にします。また、発見された問題がお客様サービスに及ぼす影響や改善策について提案し、将来セキュリティ事故が起きないようなシステム改善を支援します。ツールのみではなく、高い専門性を有する技術者が手動で誤検知を除きながら、網羅性と正確性の高い検査を実施するとともに、技術者によるオリジナルの分かりやすい報告書を提供できるのもNTTデータならではのサービスです。

◎SOC・セキュリティ監視サービス

標的型攻撃検知サービス「PatoLogphin®」	プロキシログの分析により、ウイルス対策ソフトやファイアウォール、IDS/IPSといった、既存のセキュリティ製品では検知が難しかった、オフィス環境に対する標的型攻撃(マルウェア感染)を検知するサービスです。マルウェア感染前の感染準備フェーズからの検知が可能なため、情報漏えい等の実害が発生する前の検知・対策実施も可能になります。サービスの導入に際して、新たにセキュリティ製品を購入する必要がないため、すぐに利用を開始することができます。
SOCサービス	セキュリティ総合監視サービス(Managed Security Service)では、IDS/IPS、ファイアウォール、DBファイアウォール、Webアプリケーションファイアウォール(WAF)等を総合的に監視運用します。監視、故障対応、検知アラートのアナリストによる監視・分析、月次レポート報告等、専門スタッフが引き受けます。Webトラフィックやメールトラフィックからマルウェアを検出するサンドボックス型の未知マルウェア対策システムや標的型攻撃検知サービスとの組み合わせも可能です。

SIEM導入・構築支援サービス	SIEM(Security Information and Event Management)によるセキュリティ情報イベント管理ソリューションで、統合的、相関的にログを監視・分析することで、セキュリティ機器単体による監視では把握できなかった潜在リスクをあぶり出します。300を超えるデータソースをサポートし、アプリケーションデータやプロトコル異常、データベースのアクティビティを監視。ルールベース、リスクベースによる高度な相関分析を行って、脅威の可視化による迅速な状況認識と脅威識別を可能にします。

◎インシデントレスポンス支援

CSIRT構築支援サービス・運用支援サービス	万が一インシデントが発生してしまった際の備えとして、ダメージコントロールと早期回復を目指すCSIRT(Computer Security Incident Response Team)の構築・運用を支援します。NTTデータの豊富なCSIRT構築運用経験をもとに、体制の定義・構築やセキュリティに関する情報提供など、お客様の組織に適したCSIRTの構築と運用を実現します。また、対外的にCSIRTを公表することで、外部のCSIRTとの連携を促し、有益な情報の共有が行えるようになるといった効果もあります。
フォレンジック・ラボ	フォレンジックに関わる技術開発を推進するとともに、フォレンジックが必要となったお客様への支援を行うのがフォレンジック・ラボです。フォレンジックに関する学術的な最新動向調査をもとに、お客様の要望に応じて、ツールを利用した証跡の収集・報告、マルウェアの解析、製品のログ解析などを提供します。マルウェアに感染させて挙動を解析したり、各種セキュリティ製品が攻撃に対してどのような挙動を示すかを検証するための環境(Honeynet)も保有しており、フォレンジック精度のさらなる向上に貢献しています。
セキュリティ・インシデント救急サービス	セキュリティ・インシデント発生時の初動対応から本格対応、被害極小化まで、一連の流れに合わせてアドバイス等によりオンサイトで支援します。緊急受付時には電話やメールで初期アドバイスを提供。その後、オンサイト初動対応で発生状況の調査や被害拡大防止のための指示を行い、本格対応として原因究明や対策計画の策定と実施、さらには被害からの回復、再発防止までをトータルで支援します。より適切な対応を実現するためのセカンドオピニオンとしても活用いただけます。