NTTデータ

脅威やリスクから企業・官公庁の活動を守るIT基盤セキュリティ対策

セキュリティを総合的に支援する「VANADISセキュリティ」

2008年3月期に施行される金融商品取引法対応や情報漏洩対策、事業継続性の確保など、企業および官公庁では、これまで以上に高度なセキュリティ対策が求められている。また、ネットワーク環境の進化や様々なコミュニケーションツールの登場に伴い、強靭かつ俊敏なIT環境への変革が進む一方で、「システム間での連携がスムーズにできない」、「予期せぬセキュリティホールが発生してしまう」など、健全なセキュリティ基盤を実現することが難しくなってきている。このような課題の解決に向けて、豊富なSI実績を持つNTTデータは、「人・組織的管理」、「情報セキュリティ」、「物理セキュリティ」を連携させたトータルセキュリティソリューション「VANADIS（バナディス）セキュリティ」を提供している。

VANADISとは、高度化・複雑化が進むシステム課題に対して、「人・モノ・運用」を統合的に管理するマネジメント基盤を核に、企業や官公庁のIT基盤を統合管理するトータルソリューションの総称である。このVANADISのラインアップの強化・拡充の一環として発表されたのがVANADISセキュリティである。

VANADISセキュリティは、内部統制強化や情報漏洩防止、事業継続（BCM）支援、オフィスセキュリティ構築等の各種セキュリティサービスを提供しながら、コンサルティングからシステム構築・運用、外部監査までをトータルにサポートすることで、安心かつ安全なセキュリティ基盤を実現していくソリューションである。このVANADISセキュリティのソリューションの特長について、㈱NTTデータ ビジネスソリューション事業本部セキュリティサービスユニット長の年清昭彦氏は次のように語っている。

「VANADISセキュリティは、セキュリティソリューションを1つ1つ導入していくのではなく、導入するセキュリティ対策を連携させて、セキュリティを相乗的に強化させます。例えば、ICカードを用いたIDによる入退管理からアクセス管理、ログ管理等のセキュリティ連携により、セキュリティを強化することができます。このIDに代表される人的情報、ITリソース、運用に関する情報を一元的ポリシーにて管理することで、IT環境を“部分最適”から“全体最適”へ変革させて、内外の脅威から企業および官公庁の活動を守っていきます。」

㈱NTTデータ
ビジネスソリューション事業本部
セキュリティサービスユニット長
年清 昭彦氏

以下では、VANADISセキュリティをベースとしたセキュリティ対策として、セキュリティ投資対効果を考慮した「セキュアWebアプリケーション構築サービス」と、セキュアIDC「SecureFort（セキュアフォート）」を紹介する。

上流から下流工程において、適時適切な対策を実施する「セキュアWebアプリケーション構築サービス」

Webアプリケーションの脆弱性を設計、製造の段階からなくしていく

昨今、不正なデータやコードをWebリクエストとして攻撃対象に送り込み、Webシステムからの情報漏洩やサイトの改ざん、サービスの停止などを狙う攻撃が頻発している。このような攻撃を防ぐためには、ファイアウォールなどの後付の対策では対処できず、Webアプリケーションの開発時やバージョンアップ時に脆弱性を生じさせないことが重要である。現在よく使われているWebアプリケーション診断ツールは、使いこなすことが難しく、開発したWebアプリケーションの試験時に脆弱性を検出できたとしても、リリース直前のため改修できないことも多々ある。NTTデータが提供している「セキュアWebアプリケーション構築サービス（以下、セキュアWebAP構築サービス）」は、Webアプリケーションの脆弱性対策を開発工程の上流から行うことで、Webアプリケーションの安全性を確保していくサービスである。その詳細は次のとおり。

●設計支援：設計書やコーディング規約のレビューを行い「設計時に盛り込むべき観点が抜けていないか」などを確認する／設計や製造時に活用できる「チェックシート」を提供する／ユーザーに最適なセキュリティ対策を網羅した「ガイドライン」を作成する。

●製造：Webアプリケーションのセキュリティに長けたプログラマが製造を行う。

●診断：Webアプリケーションが安全かつ安定したつくりになっているかを主に試験時に診断する。また、開発環境に対しても同時に診断する／オプションとしてソースコードレビューの診断を行う／下流工程にあたる運用や改修時に定期診断を行う。

以上のようなサービスとともに、次に示すツールを活用して、正確・的確なセキュリティ対策を行っていく。

◆SecureBlocker（セキュアブロッカー）：Webアプリケーションの脆弱性に対して効率的な対策を行うことが可能なライブラリ（Javaおよび.NETに対応）を提供。これによって製造時の実装エラーを防ぐとともに、アプリケーションの実行時に入力データの検証を行い、不正なデータが入力された場合にエラーとすることで、アプリケーション全体に一律のWeb脆弱性対策を可能にする。

◆Web Application Firewall（WAF）：正当なWebリクエストを装ってファイアウォールをくぐり抜けてくる攻撃をブロックするツール。あらかじめ定義した正当なデータから外れるリクエストや、あらかじめ定義した不正なデータに該当するリクエストをブロックすることに

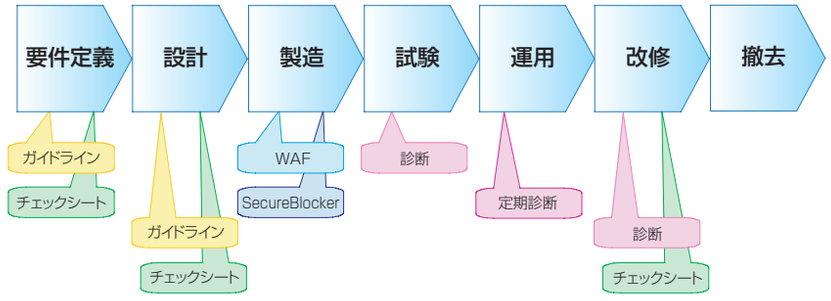

図1　開発工程とセキュアWebアプリケーション構築サービスの概要

分類	設計No.	見出し	確認項目	補足説明	キーワード	必・推区分	設計適用	適用対象範囲	適用変更理由
1 データ保護・ユーザー認証									
	1.2 ユーザー認証								
	D-1	アカウントロック機能	アカウントロック機能・クライアント特定機能を実装する	アカウントロック機能が実相されていない場合、ツールによる総当り攻撃が容易になる クライアント特定機能が実装されていない場合、不正アクセスの解析が困難になる	・認証処理の作成／変更	必須			
2 アクセス制御・セッション管理									
	2.2 セッション管理								
	D-2	URLによるセッション管理の禁止	URLには、セッションIDを含んではいけない	URLに含まれる情報は、Referer、Webプロキシサーバのログ、ブラウザの履歴などに記録されるため、セッションIDが漏洩してしまう	・セッション機構の作成／変更 ・セッションの利用	必須			

図2　設計チェックシート例

より、様々な攻撃をWebアプリケーションの手前で防御する。

◆ログ強化ライブラリ：ログ強化を可能にするライブラリを提供して、セキュリティインシデントが発生した時の調査を効率よく行えるようにする。

専門スキルを持つ技術者が適時適切な対策を提供

現在、Webサイトへの対策として、一般的にはOSやWebサーバを対象としたネットワークセキュリティ診断が行われているが、Webアプリケーションへの具体的な対策は、十分に行われていないのが現状である。また、セッション管理の改修はWebアプリケーションの根幹にかかわるため、大掛かりになることが多く、費用や期間を増大させてしまう傾向にある。このような問題を解決したセキュアWeb AP構築サービスの特長について、㈱NTTデータ ビジネスソリューション事業本部セキュリティサービスユニット セキュリティビジネス担当 課長代理の入宮貞一氏は次のように語っている。

「セキュアWeb AP構築サービスは、Webアプリケーションの安全性と信頼性を高めることを目的としています。そのために、開発工程の上流から下流にかけて適時適切な対策を提供します。例えば、必要な対策が要件から漏れるのを防ぐためのガイドラインやチェックシート、製造時の実装エラーを防ぐためのライブラリなどがあります。ガイドラインに基づいて対象となるアプリケーションに必要な対策を検討し、必須な項目をチェックシートに盛り込みます。これを設計や試験時に活用することでセキュリティを高めます。さらに、製造と診断をセットにすることで総コストを抑えることも可能です。加えて、お客さまの要望や予算、システムに合わせて重要と思われる箇所のソースコードを診断することもできるので、ツール診断では検出しにくい認証関連やセッション管理の脆弱性などを的確に診断できます。」

セキュアWeb AP構築サービスは、従来の診断ツールではなく、高い専門スキルを持つ技術者が中心となった、診断ツールでは検出できない脆弱性を実際の動作状況等を参照しながら手操作で確認して、診断のレベルと信頼性を高めていく。具体的には、はじめに診断対象に関するヒアリングを行い、診断ツールと手操作やソースコードで確認して、正確・的確に診断する。そして、検出された脆弱性の内容を整理して、報告書を作成し、問題点の解析を行っていく。NTTデータは、この診断サービスをパートナー企業のNTTデータセキュリティ㈱と共同で行っている。

㈱NTTデータ
ビジネスソリューション事業本部
セキュリティサービスユニット
セキュリティビジネス担当　課長代理
入宮 貞一氏

システム運用からセキュリティ対策まで、一貫したトータルサービスを提供するNTTデータの「セキュアIDC」

システム運用とセキュリティ対策を統合して提供する「SecureFort」

インターネットを活用したビジネスを展開している企業において、システム運用とセキュリティ対策は、ビジネスへのリソースを割かれることと、24時間365日の運転を管理するということから、特にコスト面で大きな負担となっている。そこで、最近では“早く・簡単に・安く”システム運用とセキュリティ対策を行うために、IDC（インターネットデータセンター）を核としたアウトソーシングサービスを利用する企業が増えている。主なIDCは、ファシリティの整ったマシン室でユーザーのサーバを預かり運用する「ハウジング」と、IDC側で用意したサーバやアプリケーション等の機能を提供する「ホスティング」、そして、ネットワークやサーバの運転を24時間365日監視する「オペレーション」などのサービスを提供している。しかし、企業のIT環境やIT戦略に応じて、ネットワークの安全性やシステムの品

質などを確保する「マネージドサービス」については、各企業が独自に取り組んでいるのが現状である。

NTTデータが提供しているセキュアIDC「SecureFort（セキュアフォート）」は、各企業のニーズに応じて、システム運用とセキュリティ対策を提供するアウトソーシングサービスである。システム部のネットワーク設計・構築のサポートから、不正アクセスの監視やサーバおよびネットワーク機器の検査等のセキュリティ対策、サーバの保守・監視・診断などを一貫したトータルサービスとして提供し、企業のビジネス展開をサポートしていく。

高度な知識と経験を持つ管理者が万全の診断・監視サービスを実施

㈱NTTデータ ビジネスソリューション事業本部セキュリティサービスユニット セキュリティビジネス担当部長の小久保勝敏氏は、SecureFortの特長について次のように語っている。

「一般的なIDCの機能と標準的なセキュリティ対策を『共有システム部』として提供しながら、お客さまのビジネスをサポートするために、個別のニーズやコストに応じたセキュリティ対策を『個別システム部』として提供しています（図3参照）。また、セキュリティレベルを診断・検査することや、不正アクセスを常に監視してトラブルを未然に防ぐために、SecureFortには、常に高いセキュリティ環境を維持していく『セキュリティ診断サービス』と、確実なセキュリティレベルを維持していく『セキュリティ監視サービス』を通常の運用メニューとして用意し、常にセキュアなIDCを実現しています。そして、お客さまのIT環境やIT戦略に応じて、当社の豊富なSI実績を活かして、お預かりするシステムの構築や関連したネットワークの設計などを『ネットワーク設計構築サービス』として提供しています。最適な品質と高い信頼性を持つシステムをご利用いただくことで、お客さまのビジネスをトータルにサポートしていきます。」

㈱NTTデータ
ビジネスソリューション事業本部
セキュリティサービスユニット
セキュリティビジネス担当部長
小久保 勝敏氏

SecureFortのセキュリティ診断サービスとセキュリティ監視サービスについては、専門性の高いセキュリティスキルを持つNTTデータセキュリティ㈱と共同で行っている。例えば診断サービスでは、サーバやネットワーク環境に潜む脆弱性を調査することで、個々のシステムのセキュリティレベルやリスクを分析し、その結果に基づいた対策を提案する。また、システムの脆弱性を指摘するだけでなく、問題が生じた場合は、その原因を分析して、その対処策や詳細なオペレーション方法までを記述した報告書を作成するなど、網羅性と正確性の高いセキュリティ対策を実施している。

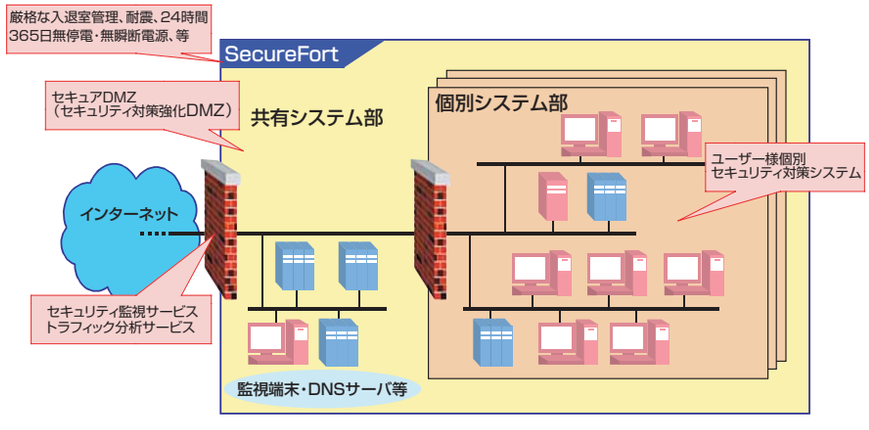

図3　システム運用とセキュリティ対策を統合したセキュアIDC「SecureFort」

お問い合せ先

㈱NTTデータ
ビジネスソリューション事業本部
セキュリティサービスユニット
TEL：050-5546-2556
E-mail：grsecure@kits.nttdata.co.jp