NTTデータ

オフィスのハイレベルセキュリティを実現する VANADIS セキュリティ

セキュリティを総合的に支援する「VANADIS セキュリティ」

企業及び官公庁では、金融商品取引法対応（日本版SOX法）や情報漏洩対策、事業継続性の確保など、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。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構築することは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実績を活かし、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」を提供する。

VANADISセキュリティは、内部統制強化や情報漏洩防止、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ている。

このVANADISセキュリティの特長について、㈱NTTデータ　ビジネスソリューション事業本部　ネットワークソリューションビジネスユニット　オフィスソリューション担当　部長の鈴木一道氏は、次のように語っている。

「企業価値向上に向けたワークスタイル変革に繋がる次世代オフィスには強固なセキュリティ基盤が必要です。VANADISセキュリティは、コンサルティングからシステム構築・運用まで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提供します。オフィスにおけるセキュリティの脅威に対し、ただ個別ソリューションを導入するだけでは不十分で、セキュリティ対策の“全体最適”を考慮したトータルセキュリティソリューションでの実現が必要です。例えば、ハイレベルセキュリティのセキュリティ基盤としては、ICカードと生体認証を用いた入退室管理、そして情報へのアクセス時の認証、情報アクセス時の操作ログ等、IDで連携を行うことで相乗的なセキュリティ強化を実現します。このID管理はVANADIS Identity Managerを活用することで一元的なユーザー管理を実現し、運用コストを低減することができます。（図1）」

㈱NTTデータ　ビジネスソリューション事業本部
ネットワークソリューションビジネスユニット
オフィスソリューション担当　部長
鈴木　一道氏

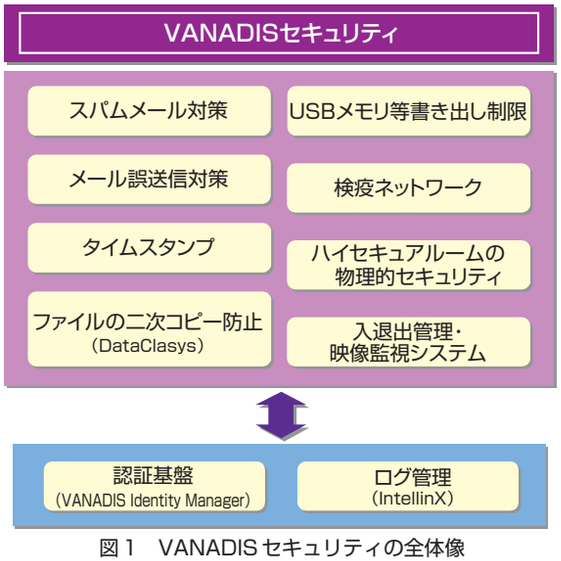


図1　VANADISセキュリティの全体像

以下では、VANADISセキュリティを用いて実現するオフィスセキュリティのソリューションとして、オペレーションログを追跡・監査する「IntellinX」と、あらゆる電子ファイルを機密度別に自動暗号化することで意図しない人への情報流出を防止する「DataClasys」について紹介する。

NTTデータ

内部統制強化に威力を発揮する「IntellinX」

内部統制の強化や情報漏洩、個人情報保護の観点から、操作ログの収集・保存・検索・監査・追跡が必要とされている。しかし、「ログを収集・一元管理し、監査することによって情報漏洩の抑止と早期発見を行うとか、ログを追跡して情報漏洩の経路や原因を迅速に特定するためにはいくつかの課題があります。」としたうえで、㈱NTTデータ　ビジネスソリューション事業本部　ネットワークソリューションビジネスユニット　オフィスソリューション担当課長の清原学氏は、次のように語る。

「大きく3つの課題があげられます。まず1つ目は、必要なログを生成するためには、業務系システムからWeb系システムまで、既存のシステムに手を加える必要があり、コストがかかるという点です。次に、ログを一元管理するためのフォーマットや送信手段の統一がなかなか難しいという点があげられます。3つ目は、ログの収集・保存だけでなく、操作を監視して日々のチェックを行い、予兆を発見するためには運用作業が必要になるという点です。特に内部統制では異常がないこと（不正操作が行われていないこと）を定期的にレポートすることが求められています。」

こういった課題を解決するため、VANADISセキュリティの新たなラインナップとして提供するのが「IntellinX」である。NTTデータが提供する内部統制、セキュリティ管理ソリューション「IntellinX」は、セキュリティ先進国イスラエルのIntellinx社が開発した最先端のオペテーションロギング・分析ソリューション（米国特許出願中）だ。

「IntellinXは、既存のサーバやクライアント端末に対する特別な設定や、新たにソフトウェアを追加する必要はなく、ユーザーオペレーションの記録・再生、不正操作の検知と警告が行えるというのが最大の特長です。図2に示すように、IntellinX用PCサーバをネットワークスイッチに接続し、メインフレームやAS400、Webサーバのパケット情報をキャプチャー（スニッフィング）することにより、ユーザーオペレーションを記録・保管します。また同時に、ビジネスルールに基づいて不正操作を検知し、警報を出すことができます。パケット情報をキャプチャーして、セッション単位で管理し、画面内容とその遷移を再現することができます。これにより、多種多様なログを統合的に追跡・監査することができ、内部統制の強化を図ることができます。」（清原 学課長）

㈱NTTデータ　ビジネスソリューション事業本部
ネットワークソリューションビジネスユニット
オフィスソリューション担当課長
清原　学氏

IntellinXの主な機能を以下に示す。

①オペレーションログ・再生機能

IntellinXサーバをネットワークに接続すると、全セッションのロギングを開始する。IntellinXの内部DBに記録されたログは、直ちに検索、参照することができる。選択したセッションは、ユーザーの操作どおりに再生（連続、コマ送り再生）することができ、サーバからの出力デー

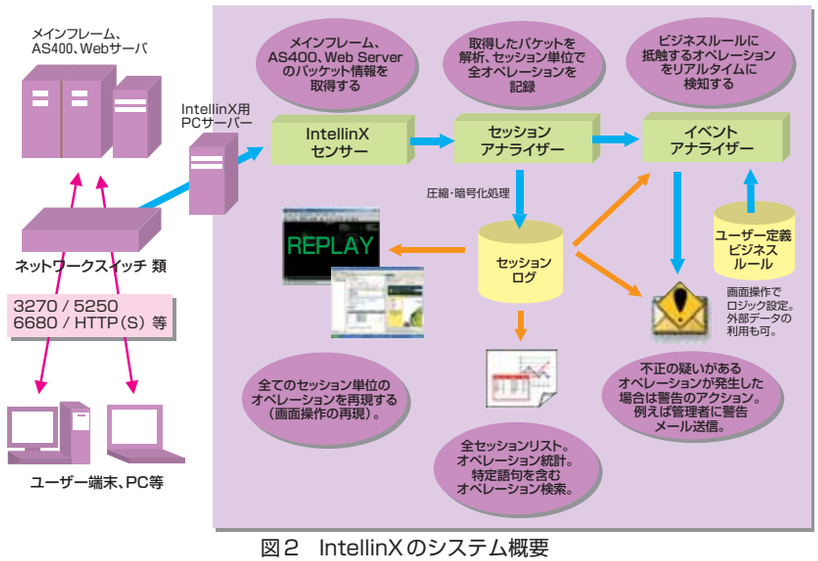


図2　IntellinXのシステム概要

図３　操作の記録・再生画面例

タ、クライアント側からの入力データの詳細が同時に表示される。これにより、何時、誰が、どの端末から、どういったアプリケーションを起動し、どういった操作を実施したのか、といった情報を検索、分析、統計処理することができる。ログは、外部メディアにアーカイブし、後日リロードすることで過去に遡って処理することが可能である。また、CSV形式等で出力することも可能だ。

②ビジネスイベント設定・通知機能

IntellinXは、不正操作をリアルタイムに検知するルールエンジンを搭載。定義した社内のビジネスルール・システムオペレーションルールをビジネスイベントとしてインタラクティブに設定することができ、ルールに抵触したオペレーションを検知すると、リアルタイムに警告メッセージを管理者に送信することができる。また、過去の操作ログを検索して、ビジネスイベントに抵触するセッションを洗い出すこともできる。

ビジネスイベントの設定は、単純なキーワード抽出からアプリケーション、オペレータをまたがる複雑なルールまで適用可能である。条件設定は、項目の相互演算やJava Scriptライクな言語を利用して設定することも可能なほか、外部データ（例えば株価データ、送金情報等）を読み出して条件に加えることも可能だ。

IntellinX用サーバは、Windows Server、及びLinux等のオープン系OSで稼動する。DBはMS SQL Server、Oracle等の一般DBで対応。また、オペレーションログの圧縮保存・暗号化もサポートしている。

このように、IntellinX は既存システムに手を加えることなく、導入も容易で、ユーザーオペレーションを記録、リアルタイムに監視し、不正行為があれば関係者に警告を発することができる最新のセキュリティ管理ツールで、内部統制強化に即効力があるソリューションといえる。

機密管理と情報共有の両立を実現する「DataClasys」

DataClasysは、機密性の高いデジタル文書やデータを情報セキュリティポリシーに基づいて、ファイル単位で管理・保護できる、高度な暗号技術に基づいた情報セキュリティ・ソリューションである。

㈱NTTデータ　ビジネスソリューション事業本部
ネットワークソリューションビジネスユニット
オフィスソリューション担当課長代理
田村　嘉章氏

「情報は正しく使われることに意味があります。個人情報や顧客情報、知的財産など、機密情報の 管理と情報の共有化を両立させるためには、セキュアなネットワーク環境とともに機密区分に応じたファイル単位での操作の制御が必要で、それよりもまず一貫した情報セキュリティポリシーの策定が不可欠です。NTTデータがVANADISセキュリティに新しくラインナップしたDataClasysは、ファイル形式にかかわらず、あらゆる文書をファイル単位で暗号化し、アクセス制御を実現します。これにより、個人情報保護法、不正競争防止法、日本版SOX法などのコンプライアンスに対応したファイル管理を実 現します。」（㈱NTTデータ　ビジネスソリューション事業本部　ネットワークソリューションビジネスユニット　オフィスソリューション担当課長代理　田村 嘉章氏）

DataClasysは、「機密情報ファイルの操作権限管理技術」と「ドライバによるファイル操作制御技術」の２大要素技術により、外部ファイルとのリンク、マクロなどによるファ

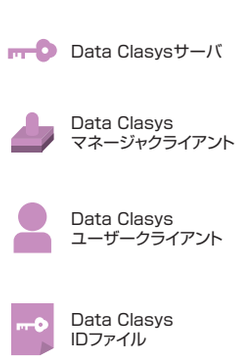
イルの操作、暗号化ファイルの全文検索など、暗号化ファイルを通常の平文ファイルと全く同じ操作で扱えるという大きな特長を実現している。

・機密情報ファイルの操作権限管理技術

機密区分別に暗号化された機密情報ファイルの利用時に、操作権限の有無をサーバで判定し、権限情報と鍵情報を配信する。操作権限の有無は、あらかじめ設定したポリシーに基づいて、利用者の所属部署や職位等の組織情報から自動的に判定するため、利用者の昇進・異動・退職等にも柔軟に対応でき、また暗号化ファイルは再暗号化等の変更を加えることなく継続して利用することが可能である（基本技術を特許取得）。

・ドライバによるファイル操作制御技術

DataClasysは、OSに独自のドライバを組み込み、機密情報ファイルに対する操作を制御する。これにより、暗号化されたファイルを一旦復号したり、一時ファイルを作成したりすることなく、暗号化されたままで通常のファイルと同じように利用することが可能である。そして、サーバから提供された権限情報に基づき、権限のない利用者による閲覧・更新・コピー＆ペースト・印刷等の操作を制限する。また、全てのファイル操作が、このドライバを通して行われるため、特定のアプリケーションやファイル形式に依存することなく、ほとんどのアプリケーションに対応している。



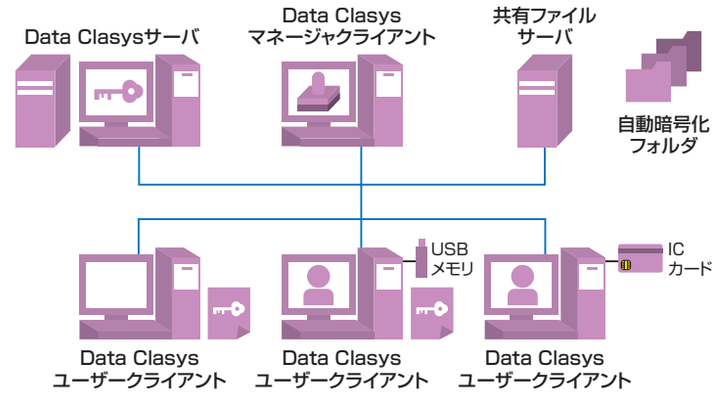


図4　DataClasysのシステム概要

DataClasysは、図4に示すように、以下の4つのコンポーネントで構成される。

- **DataClasysサーバ**：利用者の利用権限についての判断を行い、権限に応じた復号用の鍵情報などを配信するプログラムで、Windows Server、Linux上で稼動する。
- **DataClasysマネージャクライアント**：ユーザー登録、利用権限の付与、管理者権限の付与、ユーザー操作履歴の管理などを行うプログラム。
- **DataClasysユーザークライアント**：利用者のPCで動作するプログラム。
- **DataClasys IDファイル**：利用者が持つ鍵情報ファイル。機密ファイルを利用する際の本人認証などを行う。USBメモリ・トークンやICカードなどに格納することができる。

DataClasysの主な特長を以下に示す。

①機密区分に応じた権限設定

「極秘」「部外秘」など期密度に応じて、あらゆるデータをファイル単位で暗号化。部署や職位により、7つの利用制限が設定できる。

②管理ポリシーを手軽に作成

機密情報を管理するポリシーを手軽に作成することができる。

③共有サーバ内の自動暗号化

共有サーバの機密区分を指定したフォルダ内に保存。同時に、既存の共有ファイルサーバも含めた重要ファイルの自動暗号化が可能である。

以上紹介したように、DataClasysは、単に重要情報の持ち出しを制御するソリューションと異なり、情報の機密性管理を逸脱するような行為を防ぐソリューションとして、極めて有効といえる。

お問い合わせ先
㈱NTTデータ
ビジネスソリューション事業本部
ネットワークソリューションBU
オフィスソリューション担当
TEL：050-5546-8427
E-mail：secureoffice@kits.nttdata.co.jp