ソリューション・レポート

セキュリティソリューション
～システムの入口と出口を強固に守る～

コンサルティングビジネスユニット
アドバンスドソリューション構築センター
アドバンスドソリューショングループ

1．はじめに

2005年4月、いよいよ個人情報保護法の全面施行を迎える。こうした動きに合わせるかのように、昨今、行政や民間企業における情報漏洩事件が多く報道されている。内部の人間の不注意で起きたものから、外部へ情報を売り渡すという不祥事、また、犯行グループが被害企業を恐喝するという悪質な事件も発生している。結果、企業は、顧客への謝罪金などの支払による金額的な損害だけでなく、信頼性の著しい低下や、中には実質的な企業活動の停止を余儀なくされるケースなど、甚大な被害を被っている。ここで注目したいのは、企業側の管理体制の不十分さが指摘されている点だ。従来も企業は何らかの対策を施してはいたが、これらの情報漏洩事件ではその原因がほとんど特定できず、特定できた場合も管理体制のずさんさが露わになるばかりだ。

CACではこの問題の大きさを早くから認識し、顧客企業に対して、情報セキュリティの重要性の啓蒙と、対策方法の提案を行ってきている。

セキュリティ対策を考える重要なポイントとしては、「事前対策」「セキュリティポリシー」「リスクマネジメント」が挙げられる。まず、企業の情報リスクマネジメントに密接した形でセキュリティ対策の範囲や投資範囲を検討する。続いて、セキュリティポリシーとして、企業内で統一するものと個人単位のもの、および対社外の防衛手段としてのものを明確に分けて策定する。さらに、システムとして対応するものと個人の意識に依存するものも分ける必要がある。そして、これらの対策を、情報収集を行いながら事前に施すことが重要である。

本稿では、技術的な事前対策として、システムへの入口を固める認証ソリューションと、システム内から外部への出口を固めるソリューションとをそれぞれ紹介する。

2．システムへの入口を強度に固める認証ソリューション

2.1　本人認証とその課題

ネットワークから利用するシステムやインターネットを介して提供されるサービスなどでは、その利用者が本当に権限を付与された本人なのかを確認する必要がある。それにより、企業は、システム上の情報を不正利用などの脅威から守っている。これは、ほとんどすべてのシステムが保有する仕組みだ。

本人認証に用いる属性は大きく3つに分類することができる。パスワードなど本人しか記憶していないものを利用する知識属性、免許証やパスポート、実印などの本人しか持ちえないものを利用する所有物属性、そして、指紋や声紋、顔面、虹彩、静脈といった本人の一定で計測可能な生体特徴を認証要素として用いる生体属性がある。

高度なセキュリティが必要な場所では生体認証も普及しつつあるが、それ以外のほとんどでは知識属性のみを利用した固定パスワードによる認証方法が用いられている。アクセス権を持つユーザーに対して予めユーザーIDとパスワードを発行しておき、アクセス時にこの情報を入力させる、という最も単純で容易な手段だ。しかし、単純で容易なために、固定パスワードのみの認証には、盗まれやすいというリスクが伴う。盗み見したり、推測したりすることが容易なパスワードでは、第三者がなりすましてアクセスする危険性が高く、システム側ではこれを見破ることができない。結果、システムやサービスの不正利用や情報漏洩などの事態が生じてしまう。

2.2　ワンタイムパスワードでの本人認証

このようなパスワードの盗難やそこから派生する被害を回避する方法の１つに、パスワードを毎回変更して本人認証を行うシステムがある。この技術を「ワンタイムパスワード」といい、万一パスワード情報が漏洩しても悪用を防ぐことができる。ワンタイムパスワードは第三者による推測が困難で、仮にネットワーク上で盗み見された場合でも悪用することはできない。これにより、セキュリティの強化が可能となるわけだ。

ワンタイムパスワードの代表的な生成技術には、時間同期型、カウンター同期型、チャレンジレスポンス型がある。同期型は、時間や生成回数をパスワードの取得者と認証者の共通の情報として刻々と変更されるパスワードを照合する。チャレンジレスポンス型では、個人が記憶する固定のパスフレーズを予めサーバーに登録し、シーケンス番号と共にクライアント側でパスワードを生成する。

一般に、同期型でパスワードを生成・取得するためには、ハードウェアトークンが必要となる。また、チャレンジレスポンス型ではクライアント側とサーバー側双方に専用のソフトウェアが必要となる。すなわち、これらの生成技術を使うソリューションでは、セキュリティ強化の一方で、導入や運用の負荷が懸念されるわけだ。

そこで、以下に紹介するのが、新しい生成技術を利用したシンプルで導入の容易なワンタイムパスワード認証ソリューション「Mideye™（ミッドアイ）」である。

2.3　携帯電話を用いたワンタイムパスワード認証ソリューション Mideye

2001年にスウェーデンのEricsson社で開発されたワンタイムパスワード認証ソリューション「Mideye」は、ハードウェアトークンなどを使用せず、SMS*1を利用して、ワンタイムパスワードを携帯電話へ配信する。欧州で実績のあるMideyeだが、日本国内では、Mideye から携帯電話の通信事業者専用網を介したワンタイムパスワードのメッセージ配信を、CACとそのグループ会社である（株）アイ・エックス・アイが共同運用・サービス展開を行っているSpaceframe®（スペースフレーム）を利用して、実現している（図１参照）。Spaceframeはシステムと携帯電話間のSMS送受信を可能とするシステムである。

2.3.1　Mideyeで実現するシンプルかつ強固なセキュリティ

Mideyeは、ワンタイムパスワードをSMSで携帯電話にメッセージ配信することにより、他社が提供する認証ソリューションに比べ、より堅牢なセキュリティを実現している。

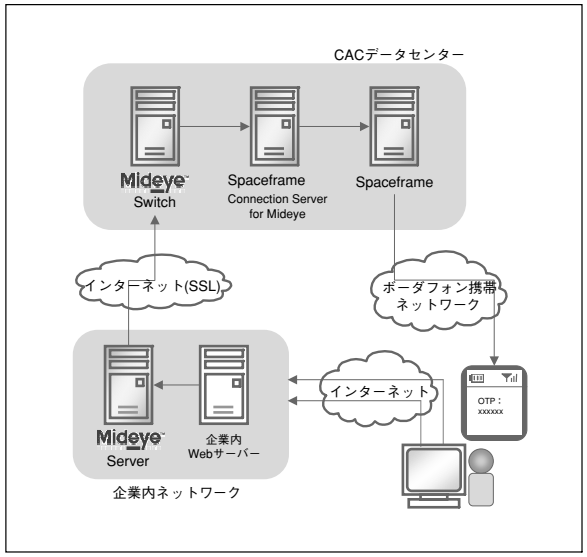


図1　Mideyeシステム構成と認証方法

ワンタイムパスワード発行の際、MideyeはPIN*2コードと携帯電話機の特定という２要素での認証を採用している。仮にユーザーIDや固定パスワードが第三者に盗まれたり推測されたりした場合でも、ワンタイムパスワードは携帯電話の所有者である本人にしかメッセージ配信されない。したがって、なりすましなどの不正アクセスは不可能となる（図２参照）。また、メッセージは、オープンなインターネット網ではなく、携帯電話の通信事業者専用網を介してSMSで配信されるため、よりセキュアな環境が実現される。

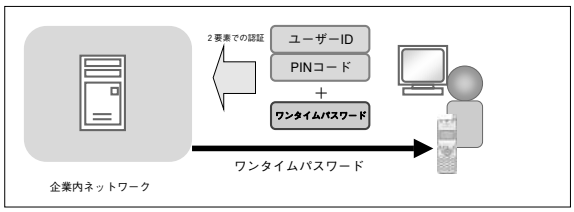


図2　Mideyeによる高セキュリティ認証

2.3.2　Mideyeのシステム構成とその認証方法

Mideyeのシステム構成とその認証方法を以下に解説しよう（図１参照）。

1）Mideyeのシステム構成

Mideyeシステムは以下で構成される。

●Mideye Server：ユーザー企業内に設置するサーバーソフトウェアで、エンドユーザー情報の管理・格納、サービス

＊1）Short Message Service：電話番号を宛先として指定することにより短い文字メッセージを送受信する携帯電話サービス。回線交換網を使用するため、遅延が少なく送達確認が可能などの特長を持つ。

＊2）PIN：Personal Identification Numberの略で、個人が持つ一意の固定パスワード。

の設定、ワンタイムパスワードの生成等を行うシステム。

●Mideye Switch：Mideye Serverが生成したワンタイムパスワードを、SMSを利用してメッセージ配信する機能を持つ管理システム。

●Spaceframe：Mideye Switchから送信されるワンタイムパスワードを、国内通信事業者の専用回線網を介して携帯電話へ送信するシステム。

Mideye認証ソリューションの利用には、エンドユーザー企業はMideye Serverライセンスの導入が必要で、Mideye SwitchやSpaceframeを介した携帯電話へのワンタイムパスワード送信はCACよりASPサービスとして提供される。

2）Mideyeの認証方法とそのテクノロジー

エンドユーザーは、クライアントPCから特定のWebサイトにアクセスし、ユーザーIDと固定パスワードを入力する。これがトリガーとなりMideye Server側でワンタイムパスワードが生成される。

ワンタイムパスワードは、Mideye Server内のランダムパスワードジェネレータで生成される。これには、共通鍵方式で商用など広範囲に用いられているDES（Data Encryption Standard）ブロック暗号アルゴリズムのOFB（Output Feedback）モードを利用している。パスワードのフォーマットは、数字（0から9）やアルファベット（aからz）、英数字（数字とアルファベットの組み合わせ）のいずれかで、4〜12桁まで設定ができる。

生成されたワンタイムパスワードは、Mideye ServerからMideye Switch、Spaceframeを介して自動的にそのユーザーの携帯電話に配信される。ユーザーが、メッセージとして受信したこのワンタイムパスワードをPC上で入力すると、Mideye Server側で確認が行われた後ログインが可能となる。

2.3.3　企業の既存環境に合わせた導入

Mideye は、LDAPインタフェースを標準サポートしており、既存のデータベースを容易に利用することができる。この場合、LDAPディレクトリには、ユーザーIDや固定パスワードに加え、携帯電話番号の情報を含むことで、Mideye Serverが受けたユーザーIDと固定パスワードの情報をLDAPディレクトリより参照し、ワンタイムパスワードの送信先となる携帯電話番号を取り込むことができる。

また、Mideye Serverは、RADIUS認証プロトコル（RFC 2865）にも対応しており、ファイアウォールやアクセスルーター、VPNルーターとの統合も実現する。

2.4　導入・運用の負荷とコストを軽減するMideye

Mideyeは既存の携帯電話を使用し、専用のハードウェアトークンやソフトウェアの導入・配布が一切不要なため、初期導入コストを削減できる。専用デバイスを使用する場合の電池交換や破損などへの対応による負荷やコストもない。また、SMSの送信は携帯電話の電話番号を宛先とするため、頻繁に変更されることが多い携帯電話のメールアドレスは管理する必要がない。

以上のように、Mideyeのワンタイムパスワード認証ソリューションは、強固なセキュリティ環境を提供するだけでなく、導入や運用にかかる負荷やコストの削減も実現する。

3．内部からの情報漏洩を防止する究極のセキュリティソリューション

3.1　内部情報漏洩の本質とは

近年発生している情報漏洩事件では、情報漏洩経路が特定されていない場合もあるが、多くが社内の人間による内部犯行と推測されている。

個人情報保護法の施行を目前にして、多くのベンダーから情報漏洩対策製品が次々にリリースされており、その具体的な対策手段は、ファイアウォール、IDS、認証、暗号化、監視などさまざまである。

では、内部犯行による情報漏洩への有効な対策方法はどんなものか。

企業によっては、「機密情報は社外に持ち出さない」といったセキュリティポリシーを設けて対応しているところもある。しかしセキュリティポリシーや対策マニュアルには強制力がなく、管理者の目の届かないところで、悪意のあるなしにかかわらず、機密情報が勝手に持ち出されているのが現状である。また、前述した各種ソリューションを導入する企業も増えてはいるが、これらの対策だけでは実際に電子データの流出を防ぎきることはできない。

本質的なことを考えるならば、「情報を社内から社外に出すことを物理的に禁止する」ことがもっとも有効なのではないだろうか。次に、それを実現するセキュリティプラットフォームを構築するソリューション「4thEye®（フォースアイ）」を紹介しよう。

3.2　情報漏洩防止・管理ソリューション 4thEye

3.2.1　4thEyeの生い立ちとその製品コンセプト

従来のセキュリティ製品の多くは、「社内の人間に悪人はいない」という「性善説」が基になっている。そのため、外部からの犯行防止を目的としたものがほとんどだった。また、内部からの漏洩防止を目的とする製品でも、外部への流出経路を完全にシャットアウトするものではない。それでは、近年多発している内部犯行による情報漏洩を未然に防ぐことはできない。

これを解決するのが、サイエンスパーク（株）が開発した情報漏洩防止・管理ソリューション「4thEye」である。4thEyeは、PCの動作を制御するドライバ層をコントロー

ルすることにより、「社内の人間が無断で情報を持ち出すこと」を防止する強力なソリューションである（図3参照）。

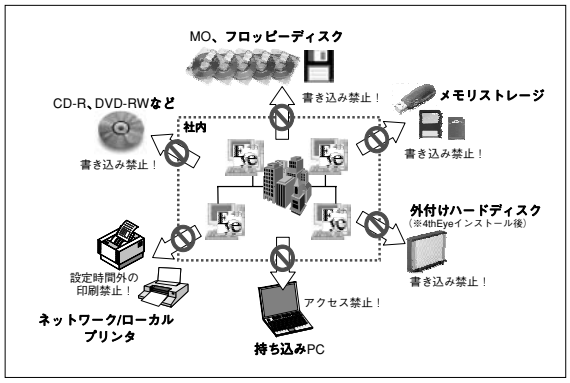


図3　内部からの情報流出をブロックする

サイエンスパーク(株)は、デバイスドライバの開発ノウハウから、OSに情報を渡すことなく、複数のドライバ間で情報のやり取りや制御を可能とするNIJI®（「架け橋」の意味を込め「虹」という名称にした）を開発、これをコアエンジンにセキュリティ製品として誕生したのが4thEyeである。

3.2.2　4thEyeの特長

4thEyeでは、ドライバ層に配置されたコアエンジンNIJIが、各種デバイス（情報が流出する経路）の監視・制御を行い、コンピュータ上に記憶されているあらゆるデータを外部ディスクへ書き出すことを禁止する。各種デバイスのドライバ層を制御するため、アプリケーションや外部デバイスの種類によって個別に対応する必要がなく、あらゆるメディアやリムーバブルディスクへの書き出しを禁止して、電子データの流出を未然に防ぐ（図4参照）。

以下は、4thEyeの特長的な機能である。

1）外部ディスクへの不正コピーを禁止

さまざまなインタフェース（IEEE1394、USB、SCSI等）を持つあらゆる外部ディスク（フロッピーディスク、MO、CD、DVD、SDメモリカード、ZIP、増設ハードディスクなど）への書き出しを一律に禁止することができる。また、他社製品では実現が困難なコマンドプロンプトからのコピーやUSBハブを経由したUSBメモリストレージへのコピーも禁止することができる。

2）持ち込みPCからのデータアクセスを禁止

外部より持ち込んだPC（4thEyeがインストールされていないPC）から、4thEyeをインストールしたPCの共有ファルダへのアクセスを禁止する。また、4thEyeをインストールしたPCから、持ち込みPCの共有フォルダへのアクセスも同様に禁止する。これにより、近年の漏洩事件で見られる持ち込みPC経由での情報漏洩を防止することができる。

3）システムロックで警告

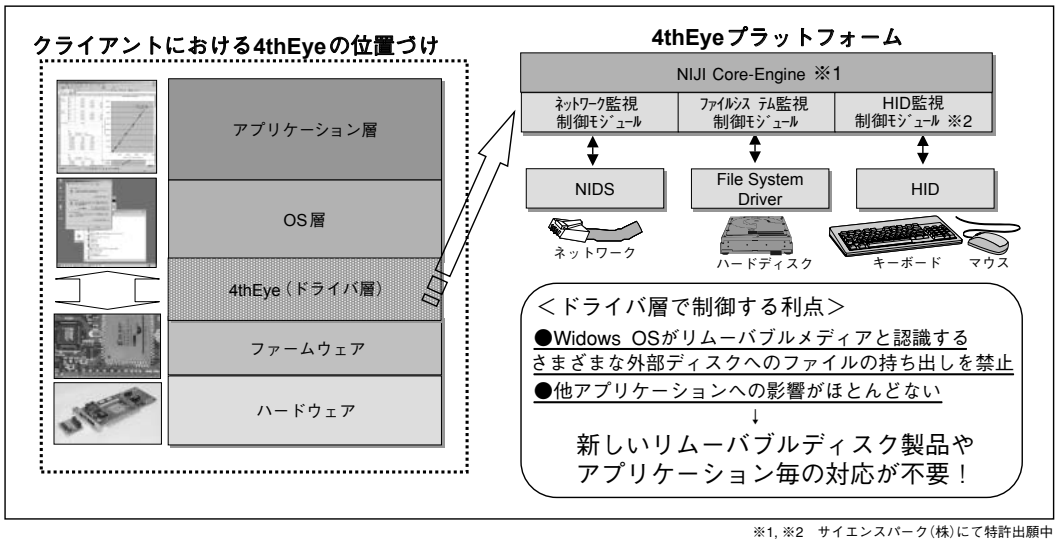
不正なコピーなど不正操作を繰り返すと、システムがロックされ、キーボードやマウスの操作が不可となる。システムロック状態は、管理者が解除しない限り、電源OFFや再起動を行っても維持される。

4）印刷行為を制御

プリンタの印刷可能な時間を設定でき、業務時間外の不正な印刷行為を禁止する。許可時間内は、「誰が」「いつ」「どのPCで」「どのプリンタから」「何を印刷したか」などの詳細な履歴を保存し、印刷媒体での企業情報の持ち出しを管理することができる。

5）ファイルの持ち出しを許可制に

業務上ファイルの持ち出しが必要な場合は、持ち出し申請手続き機能を利用する。簡単な操作により、管理者側は、「誰が」「いつ」「どのファイルを」持ち出すのかを厳重に



※1, ※2　サイエンスパーク(株)にて特許出願中

図4　4thEyeのドライバ層での制御

管理することができる。

6）ログ管理で流出経路を特定

4thEyeをインストールしたすべてのPCの、ファイルを開く、閉じる等のファイルアクセスログに加え、不正操作や持ち出しの申請・許可、システムロックなど、さまざまな操作ログが保存できる。これにより、機密情報の取扱い状況の把握や、万一情報漏洩が起こった場合の流出経路をトレースすることができる。

7）運用レベルに合わせた導入が可能

ネットワーク上の特定クライアントに対するアクセス権限の緩和（外部ディスクへの書き出し可、操作ログ保存）や、特定の外部ディスクへの書き出しを許可するなど、運用レベルに合わせたセキュリティレベルを設定することができる。

3.2.3　4thEyeのシステム構成

4thEyeシステムは下記で構成される（図5参照）。

●4thEyeクライアント：ユーザーの不正操作を禁止するモジュール。コンピュータ利用者のファイル操作を監視し、ファイルの持ち出し許可や不正操作、印刷ログを4thEyeサーバーに送信する。

●4thEyeマネージャ：4thEyeクライアントを管理するモジュール。4thEyeサーバーを介して、ファイルの持ち出し許可やクライアントのシステムロックの解除などの承認権限を有する。ログの閲覧も可能。

●4thEyeサーバー：4thEyeクライアントPCの状況管理やログの保存を行うサーバーソフトウェア。

すべての4thEyeクライアントとマネージャは4thEyeサーバーに接続する。

4thEyeのエンジンはカーネルモード*3で動作しており、通常のアプリケーション（ユーザーモード*4で動作するソフトウェア）と比べ、最大約100倍の速度で処理している。そのため、高スペックなハードウェアを必要とせず、導入しやすいシステムといえる。

3.2.4　業務や運用に合わせた製品ラインナップ

ここまでに紹介した4thEye製品は、ネットワーク対応製品のEnterpriseである。4thEyeには、この他にも、ユーザー企業の業務/システム要望に応じてスタンドアロンで利用できる製品ラインナップも用意されている（図6参照）。それぞれの特徴と概略は以下のようになる。

●Standard：内部情報漏洩対策の基本機能を備えた製品。あらゆる外部ディスクへの企業情報の持ち出しを禁止する。企業内の研究開発部門や中小の法律・会計事務所、会員制サービスを提供するショップなど、コンピュータ上のデータ共有範囲が非常に狭く、データを外部に持ち出す必要が一切ない業種・業務に適している。

	Enterprise	Professional	Standard
リムーバルディスクへのファイルの持ち出し禁止	○	○	○
持ち込みPCからのアクセス禁止	○	—	—
ファイルの持ち出し許可	○	○ (*1)	—
印刷時間制御、印刷ログの保存	○	—	—
ファイル操作ログの保存	○	オプション(*2)	—
PCのシステムロック	○	—	—
セキュリティレベルの設定	○	—	—
システム構成	C/S	スタンドアロン	スタンドアロン

(*1)　4thEye専用USBキーを使ったファイルの持ち出し許可
(*2)　ログサーバーを追加することにより、ログの記録が可能

図6　4thEye製品ラインナップ機能比較

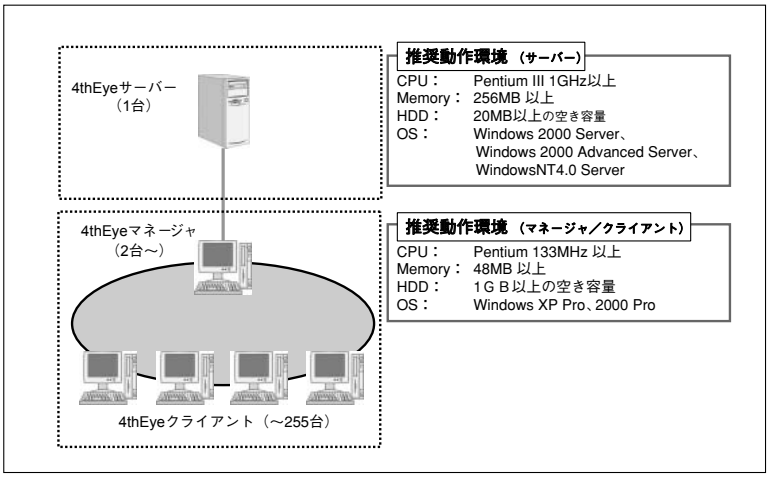


図5　4thEyeシステム構成図

＊3)、＊4）カーネルモード／ユーザーモード：システムの安全性・信頼性を維持する為に設けられたプログラムの実行権限区分。カーネルモードは、OS本体やデバイスドライバが動作するモードで、ユーザーモードは、一般のアプリケーションが動作するモード。

●Professional：Standardをベースに、データを外部ディスクへ一時的に書き込むことができる機能を追加した製品。4thEye専用USBキーをPCに差し込んでいる間のみ外部ディスクへのデータの書き込みが可能になる。また、オプションのログサーバーを追加することにより、操作ログの記録が可能になる。コールセンターや経理、人事部門などコンピュータまたはシステム上のデータ共有を限られた範囲で行い、情報を持ち出す必要がほとんどない業種・業務に適している。

●Enterprise：4thEyeの機能をフル装備した最上位版（概略や特長となる機能は3.2.2および3.2.3で述べた通り）。顧客や会員情報などを多く保有し、業務上そのデータを広い範囲で共有している企業に適している。

3.3　4thEyeによるシンプルで堅牢な内部情報漏洩対策

4thEyeは、既存のアプリケーションに影響を与えず、ユーザーモードで動作する従来のセキュリティ製品では実現が困難だったシンプルかつ堅牢なセキュリティプラットフォームを構築できる。これまでは、セキュリティポリシーや対策マニュアルなど人的な対応だけでは情報を守りきれない場合もあり、また、ファイルの個別管理を必要とする従来製品では設定ミスなどのため「いつのまにか情報が漏洩してしまった」というケースもあった。しかし、4thEyeは、一律に全てのデータ持ち出しを物理的に禁止するため、企業にとって致命的な事態を極力回避することが可能となるのである。