

米国 IT 業界の新技术紹介

- 米国における ID 技術アクセス管理 -

セキュリティ・コンプライアンスという言葉は IT 業界にとって目新しいものではありません。米国では FISMA (Federal Information Security Management Act) が 2002 年に成立し、IT システム、アプリケーション、データベースへの適用を要求されるようになっていきます。語られるよりもより困難な要件が要求されているのも確かです。多くの省庁がこの 6 年間、IDS、個別認証、情報セキュリティ、管理、監査等のツールを組み合わせ、駆使し対応の努力を重ねていますが全てを満足する状況ではないようです。

このような中、IBAC(Identity Based Access Control)= ID 利用アクセス管理が開発され、SSLVPN や NAC のような高度な認証技術と統合し、アクセスポリシー付与、管理が簡単に出来るようになってきました。

IBAC の概要

ユーザー ID を使用し ID に紐付いたアクセス制御を行なうものです。この ID とはサーバー・ルームに入る時に使用する ID バッジと同様バーチャルなデジタル・バッジを ID と呼びます。アクセスの内容を決定するのがポリシー、ポリシー付与の根拠となるものがこのデジタル・バッジということになります。

IBAC を形成するには以下のような項目が要求されます。

- 1) 企業ネットワークへのアクセス権限のある ID を定義し認証情報とすること
- 2) LDAP や AD のように、ID 及びアクセスポリシーの管理保管ができること
- 3) ネットワークアクセスの認証を行なうこと
- 4) ユーザーの全パケットに ID を貼り付けること
- 5) ID によりアクセスできるリソースの完全差別化が出来ること
- 6) NAC との統合で機体認証(ウイルス定義等のポスチャー)を行なうこと

IBAC のプロセス

FISMA と HSPD-12(米国連邦政府全体の ID 管理実行の大統領令 = FIPS201)をどのように満足するかについて簡単に申し上げます。

- IBAC を導入し多重認証(ユーザー名、パスワード、RSA 2 ファクター認証、等の組合せ)を設定し AD などポリシーを作成します。
- 認証が終了すると IBAC が PC のセキュリティ機能を検査します。
- デジタル ID をアクセス許可のあるリソースへの全パケットに付します。
- ID によるポリシー定義と付与を行ないます。

このプロセスは内部アクセス、リモートアクセス、無線 LAN 等、全ての認証されたアクセスに適用されます。2005 年にスコットランドで行なわれた G8 サミットにおいて、SSLVPN が使用されポリシーに基づくアクセス管理が行われました。選定理由は短時間でポリシーとアクセス権限の設定が作成でき、高度なセキュリティが確保できるというものでした。SSLVPN に加え IBAC で更に高度な ID+ポリシーによるアクセス管理を統合が可能になります

KK ICH 3-5-17-408 Nishigotanda, Shinagawa, Tokyo 141-0031 Japan

Phone +81-50-3735-0211

<https://www.ich-one.com>

IBAC を必要とする環境

英国の偽クレジットカードの被害は2004年の被害額に比しますと2006年には劇的に67%減少しました。Payment Card Industry Data Security Standard (PCI DSS)をクレジット、デビットカードに採用し、カードに付されたセキュリティ機能が寄与したもので、英国カード業界には朗報でありました。このような反面、情報漏洩はよりインサイダーにより引起される傾向が顕著になり、ユーザーデータや使用データがターゲットになってきました。現在ではITセキュリティの課題は内部データの、内部流出が問題となっています。これに関する監査、鑑識に掛かる費用は非常に大きくなっています。

小売業の無線LAN使用は増加しており、セキュリティ確保が課題になっています。事実、クレジットカード番号が空間を飛び交っており24時間X365日稼働を要求されます。このような情報はトランスペアレントに、システムに負担を掛けずに保護する必要があります。

ネットワーク管理者は近年、セキュリティ確保の反面、リモートアクセスより簡単にできるように求められています。取引先や顧客にネットワークを開放することで更に危険のポテンシャルは高くなります。ネットワーク管理者に対しての調査で、下記のようなユーザーに対してアクセスを許可済みか予定であることがわかりました。

仕入先、代理店 (39%)
訪問者 (28%)
外注先従業員 (36%)
契約社員 (57%)
外部ITサポート、メンテナンス(59%)
お客様 (32%)

この調査で見えてくるのはネットワーク可用性とセキュリティのジレンマです。これら相反するニーズを同時に満たすシステムの需要が急激に高まっています。サーバーとクライアントがお互いに認証し合い、データ・アクセスを制御するシステムが必要です。Windows, MAC, 小型PC, Windows CE, iPhone, iPod等は無線LANからデータ・アクセスを試みます。これらにアプリケーション層でクライアント・サーバー検証を行なう必要があります。また、旧WindowsOS, Linux, Solarisもサポートの必要があります。現在使用されている全てのブラウザにも対応しなくてはなりません。

IBAC (Identity Based Access Control) はこのようなニーズに対応できる最新のアクセス管理デバイスです。いち早くこの技術を導入し提供しているのがAEPネットワークス社の“IDpoint”が上げられます。<http://www.ich-one.com/JAEPIDpoint.pdf>

株式会社アイシーエイチ