新たなリテラシを支えるミドルウェア

--- セキュリティ機能のパッケージ化と汎用化 ---

山口英　(奈良先端科学技術大学院大学)

- **コンピュータ・リテラシの変遷**

  1990年代初頭に、それまでのプログラミング偏重型教育を改め、誰もが当たり前にアプリケーションソフトウェアを使おうというパラダイムシフトが、我が国におけるコンピュータ・リテラシの登場であった。当初は、ワープロ、表計算、プレゼンテーションがアプリケーション三種の神器であり、その利用を促進させた。90年代後半になると、電子メール、Web、P2P型コミュニケーションツール(チャット等)が、新たな三種の神器と考えられている。そして2005年の現在、我々に求められている新たなコンピュータリテラシは、単純にアプリケーションを使いこなすことではなく、セキュリティのマインドを正しく持って、コンピュータを使いこなすことにある。具体的には、暗号化、認証機能への対応、そして、データの一元管理に対応する能力を我々が身につけることだと提案したい。

- **多様化するセキュリティ機能に対する要求**

  現在の多くのアプリケーション・ソフトウェアには、セキュリティ機能が組み込まれているものの、その利用が促進しているとは言い難い。これは、セキュリティ機能を利用することがオプションと考えられているからだ。しかしこれからは、セキュリティ機能を使うことが当たり前の世界になっていかなければならない。しかし、同時にユーザに対して、セキュリティ機能を使うオーバーヘッドを与えてはならない。そのために、オーバーヘッドを隠蔽するメカニズムが必要で、よく設計されたミドルウェアとして実装されるだろう。

  また、要求されるセキュリティ機能も、単純な暗号化処理から、さまざまな認証処理、ユーザの利用状況の監査、システムの健全性確認などのさまざまな機能が必要になる。これらの機能をできる限りパッケージ化し、ユーザのオーバーヘッドを最小にして使えるようにすることも必要だ。

- ## 自己識別とコンテキスト

  ネットワーク環境でのセキュリティ、特にユービキタス環境のような境界線がきわめて曖昧な環境を考えると、改めて「自分自身はいったい誰なんだ」という自己識別の機能を充実させる必要がある。現在の多くの認証システムでは、特定のアカウント名と、それに対応づけられたパスワード（PIN）への一致を検査することで、本人確認を行っている。しかし、この機能は弱いと考えられつつある。生体計測を用いたより強力な自己識別機能の実装が求められており、その利用も広がりつつある。また、同時にネットワーク環境において広く利用可能なシステムでなければならない。

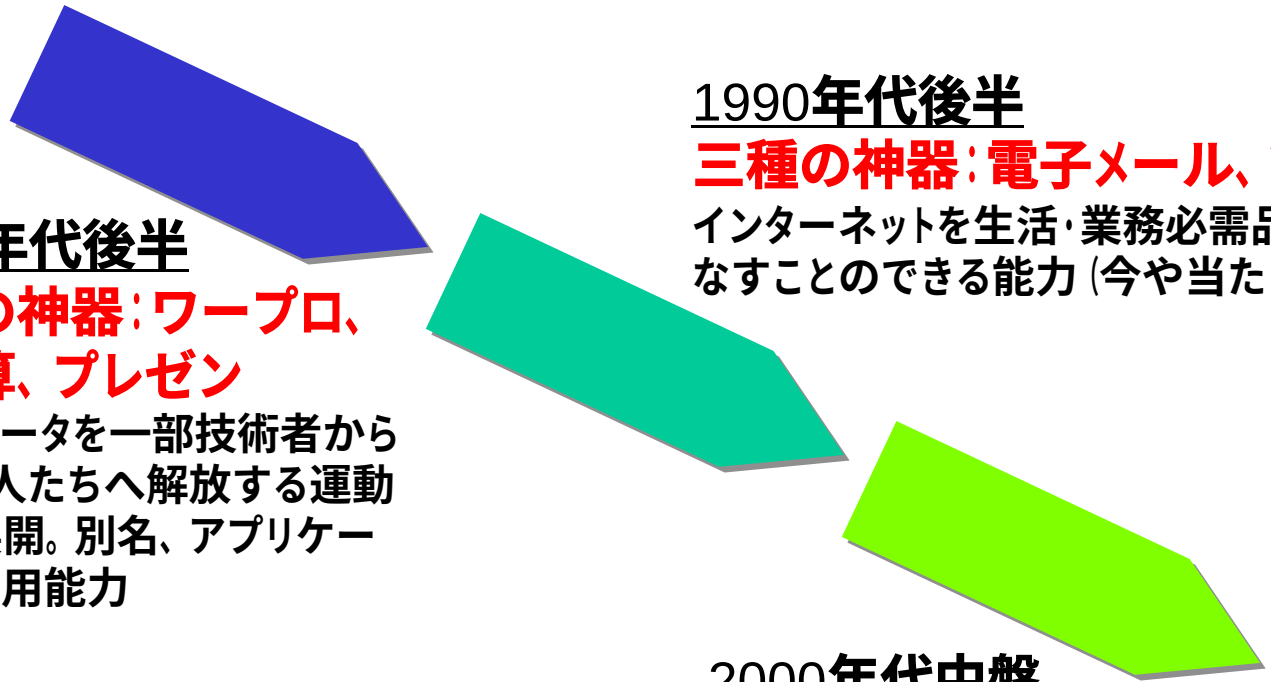
  また、自己識別が正しくできたとしても、その先でサービスなどに対するアクセスには、利用のコンテキストを評価した結果として実現されるべきだろう。そのためにはRBAC (Role Based Access Control) などの技術を適切に利用できるようにし、セキュリティ管理に「コンテキスト」の概念を導入することが必須である。

  これらの機能は、ミドルウェアとして実装され、簡単に使えるようになっていかなければならない。また、ミドルウェアそのものの構成でも、tamper free memoryをどのように実装するのかというような課題も解決する必要がある。

- ## 分散の力と集中の利点

  現在のネットワーク環境は、祖結合分散処理環境と呼ぶことができる。これは障害にも強く、また、資源の効率的な利用も期待できる。一方、情報資源にしても、制御系も分散していることから、何らかのポリシーを強制する (policy enforcement) 機構を作り出すことが難しい。このため、最近、ネットワーク環境でありながら、キーとなるサービスは集中型で管理をするような形が一般的になり始めている。このような、新たなネットワークアーキテクチャ（サービスアーキテクチャ）についての探求と、そこへのセキュリティ機能集約が必要になってきた。どのようなアーキテクチャとすべきかという議論は、今後も必要であり、同時にその実装を通して妥当性検証が必要になっている

Computer Literacyの変遷



1980年代後半

三種の神器：ワープロ、表計算、プレゼン

コンピュータを一部技術者から一般の人たちへ解放する運動として展開。別名、アプリケーション活用能力

1990年代後半

三種の神器：電子メール、Web、P2P

インターネットを生活・業務必需品として使いこなすことのできる能力（今や当たり前）

2000年代中盤

三種の神器：暗号、認証、データ管理

情報資産管理を適正に行える能力を身につけることが求められる。”Sense of Security” & “Culture of Security”

Security functions are available, but….

- ほとんどのユーザがセキュリティ機能を自発的に使っていない（日本国内限定）
  - S/MIME, PGPで暗号化されたメールはほぼ皆無
  - ファイルやディスクが暗号化を自慢されたことは無い
  - サーバと暗号化通信を利用しているケースも少ない
  - VPNをまじめに使っているユーザはほとんどいない
- ネットワークの研究者はたくさんいるが、実務家でないケースがしばしば見られる
  - 感性がなまっている?

つまり…

セキュリティは、ユーザの自発性に期待しても無駄

ユーザに気づかれないよう強力な対策を実装し、
その管理運用を徹底して行っていく機構が必要

1） 統一されたモデルと制御の適用
2） 管理性、監査性を十分に考えた設計
3） 種々のアプリケーションに適用可能な設計

安直な答えは middleware　(*^_^*)

多くの挑戦が必要 (1)

- **技術集積**
  - **さまざまな認証技術を、「ネットワーク越しに利用可能にする」ためのフレームワークを考え直す**
    - **安直な答えは** PKI **だが、実際にセキュリティ管理のことを考えると、現在の**PKI**だけでは不十分**
    - Historic data management **の機能が情報セキュリティの領域では必要になってくるが、この技術・インフラが未整備**
  - **新たな暗号技術を集積する**
    - **モジュール化**
- **新たなノウハウの集積**
  - Context oriented access control (“Role based” AC: RBAC)
  - Audit Trail / Log analysis / Single sign-on
  - ….

多くの挑戦が必要 (2)

- **標準化** vs. De Facto **化**
  - IETF**での**GSSAPI**標準化はとてつもない努力が必要だった**
    - Kerberos 4/5**の利用促進にはつながった**
    - **しかし、汎用的なインタフェースかというと、疑問が残るところもある**
    - **膨大な時間を必要としたことも問題**
  - **標準化プロセスを経ずに、**”de facto”**化によって対応することも検討されたことはかなりある**
    - **汎用化が難しい**
    - **特定製品のための** middleware
    - **セキュリティは特定の製品が対応するだけでは、どうしようもない**

多くの挑戦が必要 (3)

- 「集中と分散」の議論再燃
  - 分散型での環境構築
  - 集中型へのあこがれ
    - 例) Thin clientモデル再び
  - Enforcementのメカニズムをどのように考えるかがキー