オフィスシステムと情報セキュリティ——構築と運用の観点から

Office Computing Systems and Information Security—From Viewpoint of System Construction and Practical Use

山田　朝彦 A. Yamada　吉野　恭明 Y. Yoshino　安東　新 A. Ando

近年のネットワーク環境とオープンシステムの普及といった背景は，オフィスシステムを多様化し，セキュリティのニーズを高めた。しかし，セキュリティに偏ると利便性が犠牲になる傾向があるため，運用を考慮したセキュアシステムの構築が重要である。また，カバーすべき技術範囲の広さと“絶対”のないセキュリティ対策の性格から，セキュアシステムの構築にはコストがかかる。効率改善のためには，設計・構築・運用を考慮し，さまざまな要求にこたえられる汎(はん)用的プロトタイプの策定が重要である。その一例として，DCE (Distributed Computing Environment) を基盤とするセキュアWWW (World Wide Web) システムを作成した。DCEの保護の下で，オフィス内部・外部のネットワークに対するきめ細かなセキュリティが実現する。

With the recent growth in diffusion of networked computers and open systems, office computing systems have become more diversified and require a more secure environment. However, it is difficult for system engineers to construct a secure system because a wide knowledge of security is necessary, and because consideration should also be given to ease of operation, which is often reduced when security requirements are satisfied.

Secure systems are more easily constructed by using a multipurpose prototype system that has been appropriately chosen from the viewpoints of design, components, practical use, and management. As an example of such a system, we have developed a distributed computing environment (DCE)-based secure World Wide Web (WWW) system in which all DCE security features are available for WWW systems.

1 まえがき

近年のコンピュータのオープン化とネットワーク化により，情報の電子化とネットワーク経由での情報流通・アクセスによるオフィス業務の効率向上が顕著である。しかし，情報の入手や活用が容易になった反面，電子化された情報は従来なかった大きな脅威にさらされることになった。そこで，オフィスシステムは，効率，利便性中心から，情報の安全性確保重視へとシフトしつつある。

一般にコンピュータシステムにおける脅威の発生要因は，災害，故障，過失，故意であるが，これはオフィスシステムにもそのまま当てはまる。ここではオフィスで取り扱う情報に対する故意の脅威を対象とし，それを回避することをセキュリティと定義する。

オフィスシステムではセキュリティ実現が最重要課題ではないため，セキュリティ技術を活用して脅威を回避しつつ，利便性の低下を最小限にくい止めることが，システム構築において重要である。以下，オフィスシステムのさらされている脅威，脅威からの防御の方法，安全性と利便性のバランスを保つオフィスシステムのセキュリティ，システム構築のベースとなるプロトタイプの重要性，そして，プロトタイプの一例としてのDCEを活用したセキュアWWWソリューションについて述べる。

2 オフィスシステムの多様化

従来のオフィスシステムでは，データベースや業務システムなどの単位でユーザとシステム間のアクセス制御を行うことにより，ある程度の安全性を保つことができた。ところが，情報の電子化が進み，オフィスシステムをとりまく環境は次のように大きく変化してきた。

(1) 作業環境と技術の進展　ユーザのパソコン (PC) 装備率向上と活用範囲の拡大，さらにはファイリングシステムなどの活用による情報の電子化が急増している。一方，ワークフローの電子化，情報システムの有機的な結合などにより，作業環境自体がコンピュータネットワークに適合してきた。さらに，インターネット技術などを活用することにより，簡単に情報共有システムを構築できるようになった。

(2) ワークスタイルの変化　従来オフィス内に隔離されていた情報を，PCを中心とする携帯端末機器を用いて，外出先，自宅などオフィス外でも扱えるようになった。また，電子メールの普及，データベースの公開により，ユーザが外部の人やシステムとの電子情報を交換する機会が増大した。

(3) 外部環境への適合　インターネットを利用したWWWによる情報発信が容易になった。オフィスでも，

情報発信と外部からの情報収集を目的として，外部システムとの接続の必要性が高まった。

このようにオフィスシステムの進展と多様化により，同一組織内のユーザ間の距離（障壁）を排除できたが，逆に今や外部との距離（分離帯）が消滅したと言える。そこで，オフィス内だけでなく，システムのかかわるあらゆる場所を見渡して危険防止の策を講じる必要がある。

3 セキュリティ要件と技術

広い意味でのオフィスシステムとそのセキュリティ要件を図1に示す。このようなオフィスシステムでは，本人認証，アクセス制御，データ暗号化，電子署名などの要素技術を必要とする。また，インターネット上で隔たったネットワーク間の安全な通信を可能にするVPN（Virtual Private Network）も，オフィスシステム構築にとっては要素的な技術と言える。オフィスの情報を外部に持ち出したり，外部から参照することが多くなるため，PC自体のセキュリティや盗聴・漏洩(えい)から防御する暗号通信技術も，安全なシステムを構成する上で必須(す)である。

図1における一つの特徴は，非定型情報の取扱いが増大してきていることである。すなわち，機密度の高い，いわゆる生情報が，ネットワーク上を流れたり，PCや携帯端末により外部に持ち出される機会が増加している。このような情報のセキュリティ管理は，システム管理者には困難である場合が多く，ユーザの意識に依存せざるを得ない。

セキュリティ教育の徹底やシステム監査機能の強化が必須であるが，そのコストと難度は高く，セキュリティ維持の運用の負担を軽減するシステム構築，管理機能，評価機構が重要である。そこで，セキュリティ実現時に効率良く運用を支援する次のような機能が必要となる。

(1) 柔軟性　　人・組織・業務の変更への対応
(2) 集中管理　　アクセス権設定，暗号鍵の管理，監査
(3) ユーザインタフェースの統一　　教育コストの削減と誤操作防止

4 セキュアシステム構築とプロトタイプ化

仕事のプロセスの基本は，“PLAN，DO，SEE”であると言われる。コンピュータシステムの実現も類似のプロセスを踏むと考えることができるが，セキュリティを実現する場合はより類似性が強い。要求仕様から設計し（PLAN），構築し（DO），検証して（SEE），次の設計につなげる（図2）。一般のシステムではこのサイクルは収束するが，オフィスシステムのセキュリティ実現では，コンピュータ犯罪者などの新たな脅威に対処するためのSEEからPLANに至るフィードバックは不可欠であり，このサイクルを絶えず回す必要がある。セキュリティ実現の“PLAN，DO，SEE”は，具体的には図3に示すような手順となる。

PLANの場合の手順を以下に示す。

(1) リソースと脅威の分析により守るべき範囲を決定し，セキュリティポリシーを策定する。
(2) セキュリティツールを選定し，利用方法の詳細を決定する。

これは，一般のオフィスでは，かなり難度が高く煩雑な作業となる。セキュリティ一辺倒で考えると，構築は比較

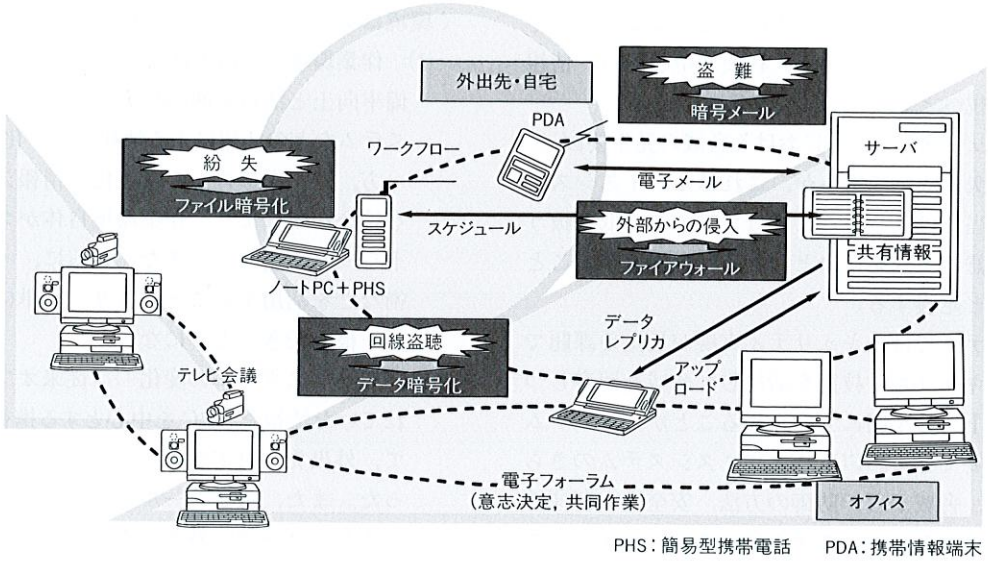

図1．オフィスシステムとセキュリティ要件　　オフィスシステムの一例と，そこでのセキュリティを実現するためのコンポーネントの例。

Office system and required security features

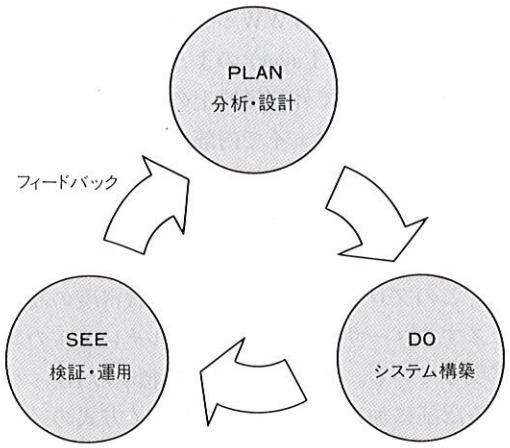

図2．セキュアシステム実現のサイクル　セキュアシステム実現においては，SEEからPLANへのフィードバックが重要である。
Cycle of secure system construction

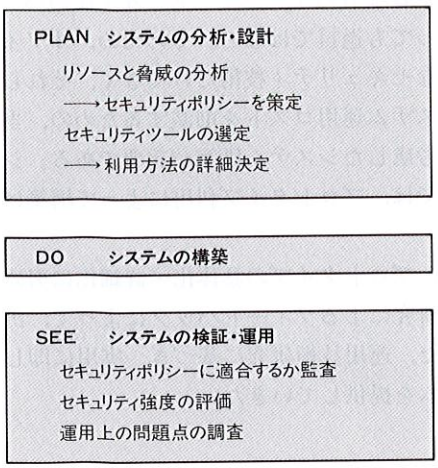

図3．セキュリティ実現の“PLAN，DO，SEE”の詳細　具体的にはこのような手順でセキュリティの実現を図る。セキュリティの観点からはSEEが特に重要である。
Details of each step of secure system construction

的容易になるが，ユーザやシステム管理者の利便性が損なわれてしまうからである。さらに，オフィスの情報のセキュリティレベルは多様である。そこで，セキュリティポリシー検討時に，情報の流通経路，情報の重要度，アクセス権の設定（人と情報）などについて，いくつかのセキュリティレベルに分類し，設定する。これには，当初からユーザ，システム管理者，情報管理者（業務・組織管理者）のセキュリティにかかわる作業を明確にし，機器，応用システムや要素技術の組合わせも加えてモデル化する必要がある。

DOでは，上述のPLANに基づいて，オフィスシステム上にセキュリティを実装する。種々のハードウェア，ソフトウェアの設定を行い，ユーザがシステムを使えるレベルにする。また，ユーザの教育もこれに含まれるであろう。

次にSEEの手順を示す。

(1) システムがセキュリティポリシーに沿って運用されているかを監査する。

(2) セキュリティ評価ツールなどの利用により，セキュリティホールを検出し，システム全体のセキュリティバランスや強度を評価する。

(3) 運用やしくみの問題点を調査する。

オフィスシステムでは，ユーザ，システム構成要素（ハードウェア，ソフトウェア，ネットワーク），組織などが頻繁に変更されるため，セキュリティの観点からは構築後の維持のためのSEEが重要である。

DOにおいては，市販のセキュリティ製品をフォローし，システムを構築するだけで多大なコストを要するのが現状である。数多くのシステムを構築する場合は，こうした作業を支援する意味で，セキュアシステムの汎用的なプロトタイプを定義することが，きわめて重要となる。いくつかプロトタイプを定義し，個々のプロトタイプをベースにバリエーションを用意することで，多種多様なシステムの構築が容易になる。さらに，プロトタイプにより設計と運用もある程度の定型化が可能であるから，ユーザ要求のより本質的な部分に対応することができる。

5 DCEベースのセキュアWWWシステム

4章で述べたセキュアシステムのプロトタイプとして，DCEベースのセキュアWWWシステムを構築した。WWWがオフィスシステムの基盤として一般化したイントラネットの重要なアプリケーションであり，そのセキュリティを後述するように基盤から考慮して実現したことが，このプロトタイプの意義である。

現在，企業ネットワークのセキュリティ対策の構成要素として重要視され利用されているファイアウォールは，ネットワークを内と外に分け，その間のデータの流れを“粗く”制御するものである。ネットワーク越しのファイル単位のアクセス制御など，よりきめ細かなセキュリティを求めるユーザに対しては，力不足とも，用途が異なるとも言える。WWWも，電子商取引システムのインタフェースとしての利用など，セキュリティが求められる状況にある。これに対しても，ファイアウォールだけで解答を与えることはできない。きめ細かいセキュリティの要求にこたえるために，セキュアWWWシステムではDCEをベースとした。

図4に，このセキュアWWWシステムのシステムアーキテクチャを示す。内部ネットワークは，DCE環境である。DCEは，異機種分散環境で相互運用性を実現することを目標にした国際標準・業界標準のミドルウェアパッケージで，PCから汎用機まで種々のプラットフォーム上でサポートさ

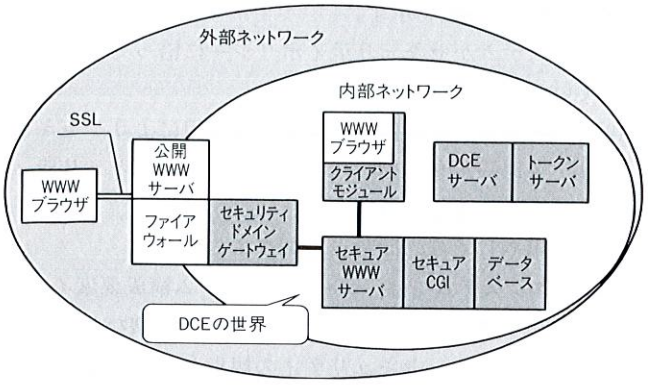

図4．セキュアWWWシステムのシステムアーキテクチャ　DCEの利用により，きめ細かなセキュリティが実現される。
System architecture of secure prototype system

れている。識別認証，アクセス制御，通信時のデータ保護，監査などの包括的なセキュリティ機能を簡単に利用でき，集中管理も可能である。このプロトタイプでは，DCE対応のWWWシステムを利用することにより，上述のセキュリティ機能の活用が可能になり，既存のWWWの課題を次のように解決した。

(1) 従来WWWサーバごとに管理していたユーザ認証用データベースは一元化される。必要に応じてシステムが代行するので，ユーザは認証プロセスを何度も繰り返す必要がない（シングルサインオン機能）。

(2) 各WWWページは，ACL（Access Control List）に基づく，より柔軟なアクセス制御が可能となる。

(3) WWWサーバとブラウザ間のやり取りは，暗号技術を用いた盗聴改ざん対策が施される。

(4) データベースなど外部プログラムとの連携に用いられるCGI（Common Gateway Interface）周辺も同様に安全対策が施される。

なお，セキュアWWWクライアントモジュールがセキュアWWWサーバとブラウザの間を仲介するので，ユーザは標準的なWWWブラウザを利用できる。

以上のように，DCEの保護の下で，内部ネットワークは安全となる。しかし，電子商取引システムにおける一般ユーザ，イントラネットにおける非セキュアセグメントのユーザなど，DCE環境をもたない外部ネットワークのコンピュータからの接続も考慮しなくてはならない。このプロトタイプでは，この課題にゲートウェイアプローチで対応する。外部からセキュアWWWシステムにアクセスする場合，SSL（Secure Sockets Layer）のようなインターネットセキュリティ技術によって外部経路上のセキュリティを確保する。そして，ゲートウェイで内部プロトコルに変換し，ゲートウェイ自身が外部クライアントに代わって，認証処理などを行う。こうして，外部からも安全なアクセスが可能となる。

また，このプロトタイプでは，より機密度の高い情報にアクセスするユーザを想定して，マルチレベルのユーザ認証を実現している。すなわち，DCE標準のID・パスワードによる認証に加えて，所有物に基づく方式の一つであるトークンカード認証もサポートしている。

6 あとがき

オフィスシステムのセキュリティ実現の課題は，ユーザやシステム管理者のオーバヘッドと安全性のバランスに尽きると言っても過言ではない。そのため，オフィスシステムに必要なセキュリティ技術だけでなく，それらを利用した際のシステム運用コストを削減するための，当初から運用管理を考慮したシステム構築が重要である。システム構築の提案では，プロトタイプ利用によって構築は効率化される。

今後も，プロトタイプの具体化・詳細化に努めるとともに，事例研究によるフィードバックによって，汎用化を目ざす。また，運用技術研究に基づき，実用に即したセキュアシステムを提供していきたい。

山田　朝彦　Asahiko Yamada, D.Sc.

情報・通信システム技術研究所開発第七担当主務，理博。情報セキュリティの研究開発に従事。情報処理学会会員。
Information & Communication Systems Lab.

吉野　恭明　Yasuaki Yoshino

情報・通信システム技術研究所開発第七担当。
システム構築・運用技術の観点から，情報セキュリティの研究開発に従事。
Information & Communication Systems Lab.

安東　　新　Arata Ando

東芝アメリカ社インフォメーションテクノロジーオフィスマネージャ。ネットワークとセキュリティの分野の技術動向調査と開発に従事。
Toshiba America Inc.