〈基盤技術〉

ダイナミックコラボレーションを実現するセキュリティ技術

Security Technologies for Dynamic Collaboration

宮内　宏* 小松文子** 河津正人*** 杉浦　昌**
Hiroshi Miyauchi Ayako Komatsu Masato Kawatsu Masashi Sugiura

要　旨

セキュリティは，ダイナミックコラボレーションを実現するための重要な課題です。NECは，ダイナミックコラボレーションのセキュリティ基盤としてiBestSolutions/Securityフレームワークを構築しました。iBestSolutions/Securityの主要コンポーネントは，セキュリティマネジメント，サイバーアタック対策，統合ID管理，および情報漏えい対策です。またNECは，プライバシー保護など来るユビキタス社会で必要とされる新しいセキュリティ技術の開発も進めています。

Security is an essential issue for Dynamic Collaboration. NEC has developed the iBestSolutions/Security framework as the security basis of Dynamic Collaboration. The main components of iBestSolutions/Security are security management, cyber attack protection, integrated identity management and information disclosure management. NEC is also developing new security technologies including privacy protection that will be necessary in the future ubiquitous society.

1．はじめに

セキュリティは，コンピュータ処理資源を広範囲に共同して使用することを実現するダイナミック・コラボレーションの最も重要な課題の1つです。セキュリティ機能はシステムを保護するだけでなく新しいサービスを実現するために必要不可欠なので，セキュリティ技術はBtoBや電子政府などのシステム開発に必要です。たとえば，電子政府では電子投票，電子入札，電子宝くじの実施が予定されていますが，これらのアプリケーションは，効果的なセキュリティ技術なしには実現できません。

システム構成のなかにセキュリティホールが存在することによってシステム全体が脆弱になる場合もあるので，システムをセキュアな状態に保つためには，全体としてのセキュリティを考えることが必要です。NECは，トータルでセキュアなシステムを実現するために，セキュリティフレームワーク「iBestSolutions/Security」を構築しました。このフレームワークは，インターネットを利用したサイバーアタックなど多くの脅威からシステムを守ります。

iBestSolutions/Securityには，4つの主要機能があります。第一に，セキュリティ対策を確実に統合するセキュリティマネジメントであり，第二に，不正アクセスなどの攻撃を防止するサイバーアタック対策です。第三の機能である統合ID管理は，複数の認証分野を組み合わせる技術です。第四は，情報漏えいを防止する情報漏えい対策です。また，iBestSolutions/Securityでは，将来のセキュリティ環境に合った新技術の開発も必要です。新技術のなかで最も重要なものとして，プライバシー保護があげられます。各種のサービスで認証を実施すると，インターネット利用時のプライバシー侵害のおそれが出てきます。つまり，認証はプライバシーと相反する性質を持つわけです。NECは，認証とプライバシーが適切に両立できるようなプライバシー保護技術について研究開発を進めています。

以下では，iBestSolutions/Securityの各技術を紹介します。第2章から第5章では，iBestSolutions/Securityの4つの主要機能について述べます。第6章では，将来技術の一例としてプライバシー保護技術を紹介します。

2．セキュリティマネジメント

セキュリティ問題に対しては，様々な対策が考えられています。しかし，これらの個別の実行は効果的とはいえません。セキュリティ対策を確実なものにするには，保護対象の情報資産，脅威，保護方法を総合的に考察する必要があります。これら対策の実行をセキュリティマネジメントと呼びます。

セキュリティマネジメントは，セキュリティ対策の基本です。セキュリティマネジメントは，セキュリティリスク

＊ インターネットシステム研究所（現在，東京大学大学院法学研究科）
Internet Systems Research Laboratories（Currently, University of Tokyo Graduate Schools for Law and Politics）
＊＊ IT基盤システム開発事業部
IT Platform Systems Development Division
＊＊＊ システム基盤ソフトウェア開発本部
System Platform Software Development Division

の査定，セキュリティ方針の計画，セキュリティポリシーの策定，セキュリティ策定支援の整備，セキュリティ監査の実行などのセキュリティ対策を適切に選択し，組み合わせることによって実現されます。

セキュリティマネジメントを実行する際には，政府発行の『情報セキュリティポリシーに関するガイドライン』や『ISO/IEC 17799』，『ISO/IEC TR 13335』などの文書を参照すると便利です。また，セキュリティマネジメントを実行するには，これらの文書と標準をよく理解しておく必要があります。さらに，ITセキュリティに関する多くの知識と経験も必要不可欠です。NECはITセキュリティ分野において高い能力を培ってきたため，これらの文書や標準に沿ったセキュリティマネジメントを遂行することができます。また，セキュリティリスクの査定，セキュリティ方針の計画，セキュリティポリシーの策定，セキュリティ策定支援の整備，セキュリティ監査の実行をサポートする各種サービスも提供しています。

3．サイバーアタック対策

3.1 従来の技術

インターネットからの不正アクセスを防止し，ネットワークの安全性を確保するためのツールが，数多く提案されています。目的やセキュリティの必要レベルに合わせてツールを選択し，場合によってはこれらを組み合わせて使用しなければなりません（**図1**）。

しかしながら，これらのツールを個別に運用しても十分な効果は得られません。

たとえば，不正侵入探知システム（Intrusion Detection System：IDS）がインストールされていても，人間が行わなければならない多くの作業が残っています。管理者はアラートが本当の攻撃なのか単に「不審な」アクセスを検出しただけなのかを判断し，攻撃の場合は，不正アクセスを阻止するために手動でファイアウォールを再設定しなければなりません。

さらに，ファイアウォールやIDSだけでOSやアプリケーションのセキュリティホールを狙った攻撃を完全に防止するのは不可能です。最近は，Webサーバ，SQLサーバ，RPCなどの脆弱性を狙った攻撃が報告されています。このような攻撃は，ファイアウォールでは阻止できず，その攻撃方法に対しての処置を具体的に示す「署名」（一連の攻撃に一致するパターン）が提供されるまで，IDSによって検出されることもありません。

従来のセキュリティツールの大部分は，不正アクセスの阻止と侵入の防止に重点を置いており，最新の攻撃方法に対処する能力には限界がみられます。次世代のセキュリティ対策として，攻撃対象となるのを避け，侵入された場合も被害を最小限にとどめる新しい技術が必要です。

■ 強化版ファイアウォールは「トラップエンジン」を装備している。トラップエンジンは信頼性情報を用いて，疑わしいアクセスだけを監視サーバに送る。

■ アクセス監視サーバは監視エンジンを装備している。監視エンジンは，アクセスの振る舞いを監視し，攻撃時にはファイアウォールに通知することにより，瞬時に攻撃を遮断する。

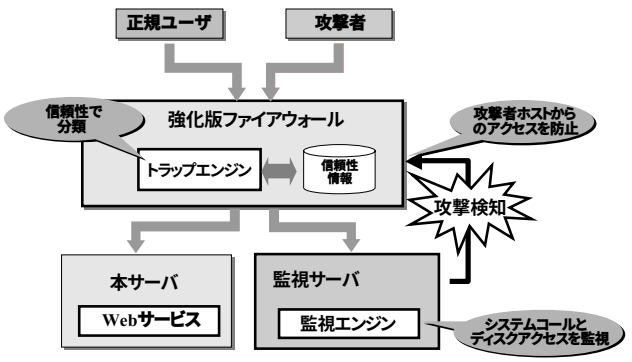

図1　ファイアウォールとアクセス監視サーバ
Fig.1　Enhanced firewall and access investigation server.

3.2 Express5800/SG300aの開発

不正アクセスの阻止のネットワークセキュリティにおける重要性は，いまだに大きなものがあり，不正アクセス防止においてファイアウォールが基本的な役割を果たすと考えられます。我々は，ファイアウォールにセキュリティ機能を追加し，これらを密接に連係させることで，ネットワーク全体を守るセキュリティゲートウェイを実現できると考えています。

NECはこのような考え方に従って，まったく新しいアプライアンスファイアウォール製品である「Express5800/SG300a」（以下「SG300a」）を開発しました。これは，ファイアウォールを中心にセキュリティゲートウェイシステムを開発し，トータルセキュリティを提供するという最終目標への第一歩です。

SG300aには，不正アクセスと侵入を防止する機能だけではなく，攻撃対象となるのを避け，侵入時の被害を最小限にとどめる機能も実装しました。具体的には，攻撃対象となるのを避けるために，以下の機能を実装しました。

・存在しないサーバへのリクエストを傍受し，サーバ応答を偽装して，攻撃者にサーバが存在すると思わせるサーバ偽装応答機能
・攻撃の対象となるのを避ける自己隠蔽機能

また攻撃の被害を最小限にとどめるために，以下の機能を実装しました。

・ファイアウォール自身を保護するホストIDS機能
・従来のIDSのように，攻撃または攻撃の準備を検出するネットワークIDS機能

本システムは，ファイアウォールのコアテクノロジとともにこれらの機能を使用して，攻撃対象ホストの検出から攻撃実行の検知まで攻撃手順の各ステップに対処します。

3.3 将来展望

NECは現在，被害を最小限にとどめるという概念を発展させて，SG300aの追加コンポーネントとして動作し，Webサーバを守る「サーバ防御システム」を開発中です。このシ

ステムは，攻撃の被害を最小限にとどめ，攻撃が続いていても正規ユーザに対しては引き続きサービスを保証します。

このシステムでは，「アクセス監視サーバ」が正規のサーバの周辺に追加されます。特定のアルゴリズムで計算される通信の「信頼性」がチェックされ，不審なアクセスはアクセス監視サーバに転送されます。アクセス監視サーバは，転送されたアクセスの動作を監視し，損害が発生したかどうかを判断します。不正な操作が何も行われていない場合，アクセス監視サーバはそのアクセスを正規のサーバに返し，不正な操作が行われた場合は，同じホストからの以降のアクセスを阻止するようにその先のファイアウォールに通知します。このアーキテクチャをSG300aと組み合わせると，正規のサーバに支障をきたさないで保つことができます。前述のとおり，OSやアプリケーションのセキュリティホールを狙ったネットワーク攻撃は増加の一途をたどっており，従来の「保護」という概念では十分には対応できなくなっています。今後は，被害の最小化と迅速な回復が基本概念となると思われます。NECは，この新しい概念とSG300aに基づいたソリューションを提供しながら，ネットワークの安全性を保つために，さらなる研究と開発を重ねていきます。

4．ID管理

統合ID管理は，認証（Authentication），権限付与（Authorization），権限管理（Administration）によって構成されるAAAの新しいソリューションです。本章では，認証とディレクトリ技術について説明します。また，NECの統合管理プラットフォームと複数の認証分野を組み合わせるID連携も取り上げます。

データ形式とアクセスプロトコルが標準化団体によって指定されているため，ディレクトリは，異なるシステム間でデータを共有するリポジトリ技術として利用されています。最もよく使われている標準アクセスプロトコルは，LDAP（Light Weight Directory Access Protocol）で，NECのEnterprise Directory Serverなど多くの製品でサポートされています。LDAPサーバでは，ID，属性，権限付与は，ディレクトリサービスに保存，管理されます。動的ID管理の要件を満たすために，**図2**に示すディレクトリ連携が適用可能です。しかし，ディレクトリ連携では，使用する組織間で統一されたポリシーと厳格な運用規定が必要だという問題があります。

ID連携は，シングルサインオンと動的アクセス制御を実現するテクノロジーです。ID連携の仕様は，Liberty AllianceおよびWS-Federationによって推進されています。NECは，2003年10月スポンサー会員としてLiberty Allianceに加入しました。**図3**にID連携のシングルサインオンの例を示します。ユーザは，IDP（Identity Provider）によって認証された後，SP（Service Provider）にアクセスできます。

4.1 認証連携

認証連携とは，存在する複数のIDPがおのおの連携することです。認証連携では，連携したIDPによってユーザが識別され，IDの属性情報によって連携先の業務リソースへの利用権限が付与されます。最近，属性情報を基づくアク

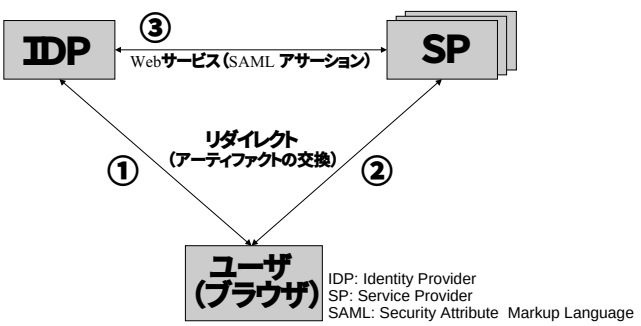

図3 ID連携の例
Fig.3 Example of ID Federation.

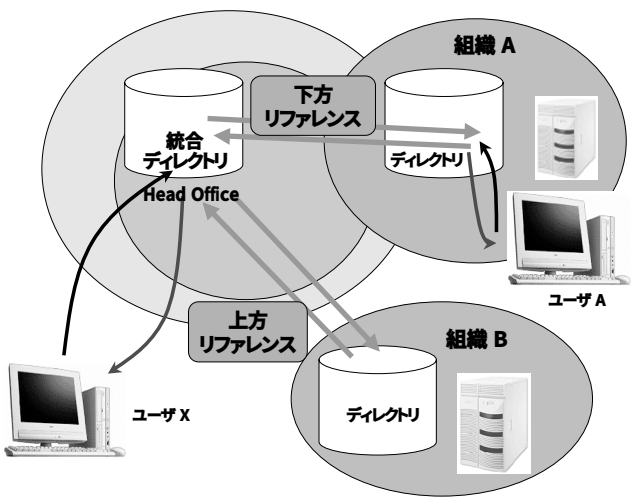

図2 ディレクトリ連携
Fig.2 Directory Federation.

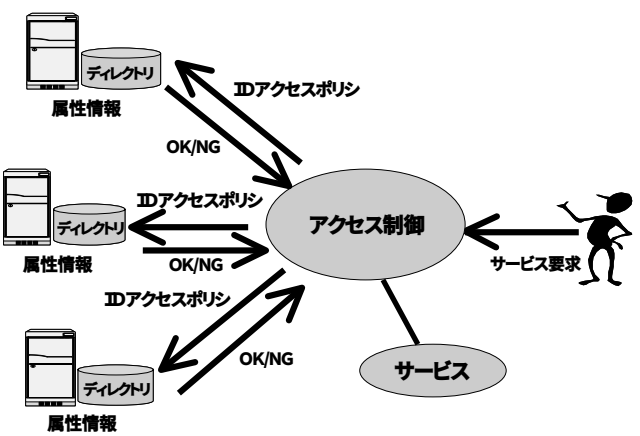

図4 分散権限管理
Fig.4 Distributed privilege management.

セスコントロールの重要性が増しており，認証連携における権限管理が必要不可欠な基盤技術となっています。

4.2 分散権限管理

権限管理では様々な属性情報を扱うため，プライバシーとの調和が求められます。分散権限管理システムは，属性情報を提示することなく，アクセスポリシーをもとに権限の有無を返します。また組織やサービスごとに管理する属性が異なる場合，属性情報は分散して管理されており，いくつもの属性情報の管理先に権限の有無を問い合わせてアクセスの可否を判定します（**図4**）。

権限管理システムにおいては，属性の格納場所を知らせる位置情報サービスや属性の変更を記録する監査機構も必要です。

5．情報漏えい対策

漏えいの80％が組織内部に起因するといわれており，そのほとんどが運用上のルールによるものだというのが，情報漏えいの実情です。また，悪意を持って行われる漏えいよりも，人的ミスによる事例が圧倒的に多く見られます。

5.1 分　類

情報漏えい対策は，**図5**に示すように分類できます。対策の効果は，抑止効果と防止効果の2つに分けられます。効果的な対策のためには，流通制限，データ保護，監視，ネットワーク防御，公示という対策が必要です。

情報漏えい対策では，特に，対策を実行することにより期待される効果を考えることが大切です。

5.2 対　策

アクセスコントロールなどの一般的な機能が対策に有効であると考えられます。図5に情報漏えい対策マップを示します。

(1) アクセスコントロール

情報漏えいの観点から，一般的なリソース，データファイル，サーバのほかに，印刷，メールへのファイル添付，および画面キャプチャも制限する必要があります。

(2) デスクトップセキュリティ

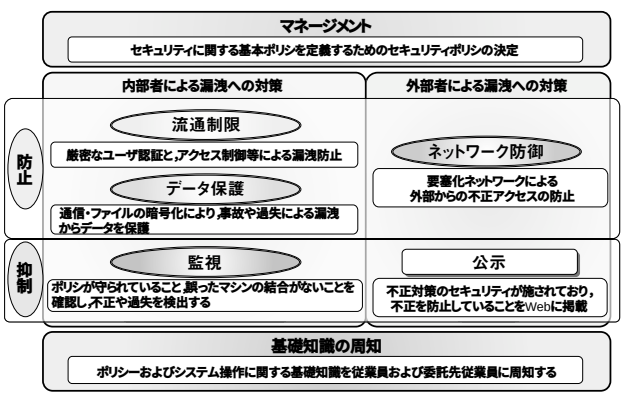

図5　情報漏えい対策マップ
Fig.5　View of measures against information disclosure.

クライアントPCの利用環境では，情報漏えい防止のための制限や保護が必要です。

(3) 異常行動の検知

ネットワークのパケット情報やクライアントPCの操作履歴から，迅速にIT資産を管理するツールを使用して，不審な行動を検出することができます。

(4) 暗号化

人による操作が情報漏えいの原因の80％を占めていることから，PCの盗難に備えてディスクやファイルを暗号化しておくことは効果的です。

(5) メール送信・Webアクセスのフィルタリング

フィルタリングは，組織内部から外部への情報漏えいを防ぐために有効な手段です。フィルタには適切なポリシーを設定するよう注意します。

(6) 監査ログ

ログの採取は，最も抑止効果のある対策と考えられています。ログ情報を監査し，監査報告に対して是正策を講じる必要があります。

6．プライバシー保護技術

第2章から第5章に述べた技術により，安全性の高いシステムを開発できます。しかし，安全性の高いシステムは，ユーザのプライバシーを侵害する原因にもなり得ます。たとえば，インターネットプロバイダは，アクセスログを参照して，誰がどのWebページにアクセスしたかを知ることができます。匿名によるアクセス方法を用いると，この種のプライバシー漏えいを防ぐことができます。しかし，この方法ではクラッカーが自分のIDを示さずにインターネットを利用できてしまうという問題があります。ここから分かるのは，緊急時の追跡可能性とユーザのプライバシー保護を両立させることが重要だということです。

本章では，2つのプライバシー保護のメカニズムを例として紹介します。まず，認証と無記名性を両立させる電子投票を示し，次に「グループ署名」というプライバシー保護のための署名方式を説明します。グループ署名の技術を用いると，通常は匿名性を保持しながら，緊急時には管理者が署名者を特定することが可能となります。

6.1 電子投票

2002年に制定された電子投票法によって，地方自治体の選挙では電子投票が認められるようになりましたが，投票は事前に決められた場所でしか行うことができません。またこの法律では，投票所と集計センタ間の電子的な通信は禁止されています。

インターネットによる電子投票では，高速で正確な集計と，投票者が任意の投票所またはインターネットに接続されたコンピュータから投票できる「場所に制限されない投票」を実現できます。一方，各投票者の投票権を確認しなければならないので，投票の秘密を守るのは困難です。

認証と投票の秘密保護の両方を実現する暗号処理方法が

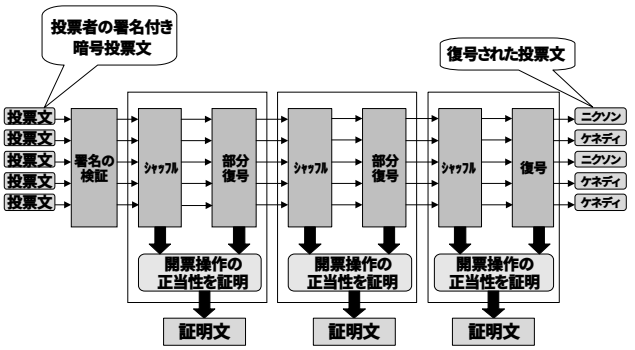

図6　ミックスネット方式による電子投票
Fig.6　Electronic voting system using Mix-Net.

いくつか開発されています[1)]。最も効果的な方式は，**図6**に示す「ミックスネット方式」と呼ばれているものです。各投票者は自分の投票を暗号化し，それにデジタル署名を付与します。投票センタは，署名を検証し「シャッフルセンター」に送ります。図6では，3つのシャッフルセンターが存在します。シャッフルセンターは，暗号化された票を部分的に復号し，票の順序を変更（シャッフル）します。最後のシャッフルセンターからは，平文の票が出力されます。シャッフルすることにより，署名された票と復号された票との対応は分からなくなり，投票の無記名性が守られます。各シャッフルセンターは，そこでの手続きの正当性を証明し，暗号化された投票の改変などの不正行為を防止します。ここでの証明には，入力された票と出力された票の対応を明かすことなく，いわば間接的に正当性を証明する「ゼロ知識証明」技術によって実行されます。NECは，集計を現実に可能にする高速のゼロ知識証明技術を開発することにより，実用的な電子投票システムを実現しました。

「digishuff-Pro」というソフトウェア製品は，この方式をもとに開発されています。

6.2　グループ署名

システム管理者によるプライバシー侵害を避けるためには，グループ署名技術が便利です。グループ署名には，以下のような特長があります[2)]。

・グループのメンバだけがメッセージに署名できる。
・署名の受信者は，その署名がグループメンバによる有効な署名であることを確認できる。
・署名の受信者は，グループのどのメンバが署名したかを特定することはできない。
・問題発生時には，署名を復号して，署名者のIDを調べることができる。

この技術により，システムのユーザは，IDを明かさずに権限を示すことができます。つまり，グループ署名を使うことにより，認証とプライバシー保護を両立させることが可能です。

ただし，グループ署名方式の管理には，メンバの管理が煩雑なこと，特にメンバがグループから外れたときにメンバ全員が自分の秘密鍵を更新しなければならないことなど，いくつかの問題点が残されています。

NECは，実際のシステム管理に合った新しいグループ署名方式を開発中です。また，メンバの署名を事前に設定された回数に制限する新しい署名方式も提案しています。この技術は，チケットサービスや電子投票などのプライバシー保護サービスに適用できると期待されています。

7. むすび

本稿では，ダイナミックコラボレーションに必要な基盤であるiBestSolutions/Securityの4つの要素技術を紹介しました。また，将来のセキュリティ環境に向けた新しい技術として，プライバシー保護技術を提案しました。NECは，これらの技術を効果的に活用して，安全なユビキタス社会を構築していこうとしています。

参考文献

1)　K. Sako, “How to Secure Network Application Systems Using Cryptographic Protocols-Electronic Voting Systems Case,” NEC Res. & Develop., 43, 3, pp.191-194, 2002-7.
2)　B. Schneier, “Applied Cryptography, 2nd edition”, Jon Wiley and Sons, 1996.

筆者紹介

Hiroshi Miyauchi
宮内　宏（みやうち　ひろし）　1985年，NEC入社。インターネットシステム研究所研究部長（現在，東京大学大学院法学研究科）。

Ayako Komatsu
小松　文子（こまつ　あやこ）　1981年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部コンサルティングマネージャー。Webサービスソフトウェア事業部，およびソリューション開発研究本部システム基盤ソフトウェア開発本部を兼務。

Masato Kawatsu
河津　正人（かわつ　まさと）　1987年，NEC入社。現在，ソリューション開発研究本部システム基盤ソフトウェア開発本部マネージャー。

Masashi Sugiura
杉浦　昌（すぎうら　まさし）　1983年，NEC入社。現在，システムソフトウェア事業本部IT基盤システム開発事業部コンサルティングマネージャー。