情報セキュリティ対策検討のために

To Plan for Information Security Measures

多田宏司, 古寺　薫

要　約　情報技術が社会インフラとなり，すべての社会活動がインターネットなどのオープンなネットワークを介して行われることで効率性・利便性が増している．一方，不正な手段，悪意を持ってネットワークからコンピュータシステムに侵入し，データを読む，改ざんする，破壊するといったような新たな危機に直面している．情報セキュリティ対策は情報資産を守るためにあらゆる組織の最重要課題のひとつとなっている．本稿では，情報セキュリティを確保するための技術要素と要求事項を整理し，各組織がセキュリティ対策を策定/実施するための指針を示すとともに最新の国内外セキュリティ技術動向の一部を紹介するものである．

Abstract　The information technology is now becoming the social infrastructures. All social activities are done across the Internet and other open information networks, and they are increasing efficiency and conveniency. On the other hand, today 's information society is faced with many new threats, such as unauthorized intentional or accidental disclosure, modification, or destruction of data in the computer systems. The information security security safeguard is one of the most important issues of every organization to protect its information assets. This paper reports technical factors and requirements to ensure the information security and presents guidelines to establish and/or enforce their security measures, and introduces some new technology trends of the information security in domestic and abroad.

1. はじめに

情報技術が社会インフラとなり経済，教育，医療などあらゆる社会活動がネットワークを利用した形態に変化し限りなく効率化・高度化が進んでいる．一方で情報や情報システムといった情報資産を守るための情報セキュリティの確保は最重要課題のひとつとなっている．情報セキュリティとは，情報資産の損失に対する抑止・予防・検知・回復などの対策を実施するための危機管理を最終目的としたシステム化の取組みである．

「情報セキュリティ」の目的は

- 「機密性」情報のアクセスを限定し，外部への漏洩を防止する
- 「完全性」情報が破壊されたり，改ざんされたりせずに，完全さを保証する
- 「正確性」情報そのものが正確なものであり，「なりすまし」などがされていない
- 「可用性」障害を防ぎ，正常の運用を維持し，利用したいときに情報が利用できる

の四つが確保できることにある．

それぞれの企業や官公庁などにおいて承認された全組織的な情報セキュリティ対策を実施するための考え方が情報セキュリティポリシーやガイドラインであり，これによりセキュリティ強度のレベルが決定されることになる．

以降，具体的なセキュリティポリシーやガイドラインを策定するための前提知識や検討項目，セキュリティ対策実施のために必要な技術要素について技術の側面とマネージメントの側面から解説する．

2. ネットワークシステムのセキュリティ

2.1 具備すべきセキュリティ機能の概要とその適用指針

情報システムにおける安全対策の一環としてネットワークシステムに具備すべきセキュリティ機能には，インターネット接続やリモートアクセスなどによって内部ネットワークが外部ネットワークと接続されることから要求されるセキュリティ強度の向上と，組織内部の利用者または他のネットワーク利用者等によるファイル，業務システム等のアクセス制御を含むセキュリティ強度の向上を図ることがある．また，セキュリティ機能を実現する要素技術，製品の変化は激しく，常にセキュリティ強度の維持という視点での運用管理作業を欠くことができない．

① 外部ネットワークに対するセキュリティ機能

インターネット，外部ネットワーク等との接続は，セキュリティを十分に考慮したネットワークシステム構成とする．

② ネットワークシステムのセキュリティ機能

ネットワーク利用者の認証を厳格に行う必要があるアクセス権管理は，利用者毎のアクセス権の設定や，個々のファイル，業務システム等のアクセス制御を可能とする．

③ 運用管理によるセキュリティ機能

アクセス履歴の収集・記録，ウイルス対策などの日々の運用管理によってセキュリティ強度の低下を防ぐ．

・ネットワークシステムを構成する各サーバは，不正アクセス，使用不能攻撃等を検出し発信元の特定のためにアクセス履歴を収集する．

・外部からの不正アクセスの原因となるセキュリティホールを定期的に診断する．外部からの不正アクセス，使用不能攻撃等を検出し外部ネットワークとの接続を遮断する．

・ネットワークシステムのセキュリティ強度に関して第三者機関による監査/認定を受ける．

・ウイルス対策については，外部から持ち込まれたリムーバブルメディア，電子メールに添付されたファイル，Web ブラウザを使用してダウンロードしたファイル等のウイルスも検出可能とする．

2.2 セキュリティ上の脅威と対策

ネットワークシステムに具備すべきセキュリティ機能の概要とその適用指針を理解する上で，ネットワークシステムに対するセキュリティ上の脅威と対策を整理しておくことは重要である．

・偶然性の強いもの（回避することは困難）

天災，故障，誤作動など

・意図的なもの（回避することは可能）

—内部での不正行為
組織の人間による不正行為
外部の人間による物理的侵入による不正行為
—外部からの不正行為
公衆網からの不正アクセス，使用不能攻撃等

上記の大分類に従いセキュリティ上の脅威を，情報システム全般にわたり，脅威の要素，発生する原因と「2.1節具備すべきセキュリティ機能の概要とその適用指針」で述べたセキュリティ機能によって実現される対策とを対応させてさらに分類した(表1).

2.3 セキュリティ対策の実装例

「2.2節セキュリティ上の脅威と対策」であげた対応策の機能概要と実装例を表2に示す.

2.4 セキュリティ対策の要点

セキュリティ上の脅威と対策の分類やセキュリティ対策の実装例に現れる，認証，アクセス制御，状況監視/診断，ウィルス対策の各技術は主要なセキュリティ技術要

表 1 セキュリティ上の脅威と対策

(1) 内部での不正行為 不必要なシステム利用、システムの破壊などの脅威がある。		
① システムに対する正当なユーザへのなりすましによる情報の漏洩、改竄		
	原因	・推測されやすいパスワードが設定されている ・パスワードをメモして貼っておく ・キーボードへのパスワード入力を覚えられる ・ネットワーク上でパスワードを盗聴 ・正当なユーザの離席時の盗聴や改竄
	対応策	・厳格なユーザ認証を行う ・スクリーンセーバ機能の使用
②不必要なアクセス許可による情報の漏洩、改ざん		
	原因	・アプリケーションや Web コンテンツ等のリソースに対して、不必要にアクセス権が与えてある
	対応策	・アクセス制御を行う
③PC の盗難による情報の漏洩		
	原因	・鍵のかかる場所に PC が保管されていない ・重要なファイルが暗号化されていない
	対応策	・重要なファイルは暗号化し、保存する ・PC の起動制限機能を導入する(BIOS パスワード、認証)
④ネットワーク上での盗聴による情報の漏洩		
	原因	・ネットワーク上を流れる機密情報が暗号化されていない
	対応策	・ネットワーク上を流れる重要なデータは暗号化する
⑤ネットワークを利用した外部への情報の漏洩		
	原因	・メール利用を無制限に許可している
	対応策	・電子メールコンテンツの監視を行い、メール利用を制限する ・ファイアウォール、リモートアクセス機能による厳格なアクセス制御を行う
⑥不必要なシステム使用による業務効率の低下、ネットワークトラフィックの増加		
	原因	・業務に無関係な Web アクセス ・私的な趣味/アダルトサイトに関するホームページの閲覧 ・私的な電子メールの使用
	対応策	・インターネット上の Web サーバ利用のアクセス制限を行う ・電子メールコンテンツの監視を行い、メール利用を制限する

表 1　セキュリティ上の脅威と対策（続き）

(2)　外部からの不正行為 コンピュータウイルス、インターネット・外部ネットワーク・電話網からの侵入・妨害攻撃、ネットワーク上での盗聴・なりすまし・改竄・否認などの脅威がある。		
	①インターネット、公衆網などネットワークからのウィルス侵入	
		対応策	・インターネット、公衆網とのゲートウェイでウイルス対策を実施する。
	②インターネットからの不正アクセス	
		原因	・インターネットから公開セグメントおよびネットワークシステムに対するアクセス制御が行われていない。 ・公開サーバのソフトウェア(Web サーバ、メールサーバ等)のレベルが古く、セキュリティホールが存在する。 ・ネットワークにどのような脆弱性があるかが事前に検証されていない。 ・不正アクセスを検知できない。
		対応策	・ファイアウォールを導入し、アクセス制御を行う。 ・公開サーバのソフトウェア(Web サーバ、メールサーバ等)のバージョンアップ、セキュリティパッチ導入などの保守を行う。 ・定期的にセキュリティ診断を行う。 ・ネットワークのリアルタイム監視による不正行為の検出及び対処を実施する。
	③インターネットからの使用不能攻撃 （完全な対策は困難ではあるが、被害を最小限に抑える）	
		対応策	・ネットワークのリアルタイム監視による不正行為を検出する。 ・ポートスキャンによって不正行為に至る事前準備の段階で不正アクセスを検出する。 ・使用不能攻撃をリアルタイムに検出し、直ちに対処を行う。 ・定期的にログを解析し、不正行為の状況を把握する。
	④電話網からの不正アクセス	
		原因	・リモートアクセス(ダイヤルアップ)でのユーザ認証が厳密でない。
		対応策	・厳格なユーザ認証を行う。
	⑤電話網からの使用不能攻撃	
		原因	・発信者の番号が特定できない。
		対応策	・登録した発信番号からのアクセス以外受け付けない。
	⑥機密データの盗聴	
		原因	・データが暗号化されていない。
		対応策	・ネットワーク上を流れる重要なデータの暗号化を行う。
	⑦通信相手のなりすまし	
		原因	・本当に正しい相手と通信しているかわからない。
		対応策	・電子署名等の暗号技術を使用して通信相手の確認を行う。
	⑧機密データの改ざん	
		原因	・受信したデータが改竄されていないことを確認する方法がない。
		対応策	・電子署名等の暗号技術を使用してデータの認証を行う。
	⑨通信の否認	
		原因	・データが本当に相手が送ったものである証拠がない。
		対応策	・電子署名などの暗号技術を使用して、相手が送ったデータであることを確認する。

素であり，これらについてその概要とセキュリティ対策の要点について解説する．

1)　認証

認証（「付録　認証技術」参照）については，現在数多くの（エンティティ）認証技術が存在する．この中でも最も普遍的に使用されているのが「記憶認証」であり，ベーシック認証とも呼ばれている認証技術である．端末のオペレーティングシステムやネットワークへのログオン時にユーザ ID/パスワードの組み合わ

表 2　セキュリティ対策の実装例

セキュリティ上の脅威	対応策	概要	実現方法	
内部不正（職員によるデータの盗難、プライバシーの侵害等）	PCへのログオン認証の強化	利用者のPCへのログオン，ネットワークへのログオンを指紋認証により行う。パスワードの管理や入力が必要なくなると同時に、他人によるなりすましが不可能となる。	・指紋リーダ（Windowsパスワード格納） ・指紋リーダ対応PCセキュリティソフトウェア	
	重要なファイルの暗号化	PC内のファイルやディレクトリの暗号化を行う。PCの物理的な盗難による、情報の漏洩を防ぐことができる。	・指紋リーダ ・指紋リーダ対応PCセキュリティソフトウェア	
	ネットワークを流れる重要なデータの暗号化	重要なWeb，メールのデータの暗号化を行う。ネットワークの盗聴による情報の漏洩を防ぐことができる。	・指紋リーダ（電子証明書格納） ・WebサーバーWebブラウザ間のデータ暗号化 ・電子メール（Outlook）の暗号化	・認証局（電子証明書発行システム）
	重要な情報のアクセス制御	利用者の権限に応じてWebのコンテンツごとにアクセス制御を行う。	・指紋リーダ（電子証明書格納） ・WebサーバーWebブラウザ間ユーザ認証	
電話回線からの不正侵入	リモートアクセスの認証の強化	リモートアクセスでのネットワークへの認証を、利用者の指紋データと暗号技術を用いて行う。パスワード（ワンタイムパスワード）の管理や入力の必要がなくなると同時に、他人によるなりすましが不可能となる。	・指紋リーダ（電子証明書格納） ・指紋リーダ対応PCセキュリティソフトウェア ・セキュア認証サーバ	
コンピュータウイルス	ウイルスの集中チェック・駆除	ネットワークを流れるデータを１ヶ所で集中的にウイルスのチェックと駆除を行う。	・インターネットサーバー用ウイルス対策ソフトウェア	
	PCでのウイルスチェック・駆除	個々のPCでウイルスチェックと駆除を行う。	・PC用ウイルス対策ソフトウェア	
不必要なインターネット利用	URLのチェック・フィルタリング	イントラネットから利用するインターネットURLのチェックとフィルタリングを行う。	・URLフィルタリングソフトウェア	
機密データの漏洩	メールの内容チェック・フィルタリング	イントラネットからのメールの内容のチェックとフィルタリングを行う。	・メールフィルタリングソフトウェア	
外部からの不正アクセス、使用不能攻撃	ファイアウォール導入	ファイアウォールにより、インターネットからの不正アクセスや使用不能攻撃を	・ファイアウォール	
	ネットワークセキュリティ監視	ネットワークを流れるデータをリアルタイムに監視し、不正なデータを検知して、管理者に通知する。	・ネットワークセキュリティ監視ソフトウェア	
	ネットワークセキュリティ診断	インターネットに公開するマシンのセキュリティ検査を行う。	・ネットワークセキュリティ診断ツール ・ネットワークセキュリティ診断サービス	

せで使用される．

記憶認証の最大の欠点であるパスワードの漏洩リスクをカバーする目的で開発された認証技術が「ワンタイムパスワード」である．これは漏洩リスクをかなりのレベルで回避することは可能であるが，クライアント/サーバ機器への当機能の組み込みまたはトークンと呼ばれるパスワード発生機構の使用が必須となる．特に後者については，トークンそのものの紛失というリスクに対応する観点でPIN（Personal Identification Number）と呼ばれる一種のパスワード（記憶認証）を併用することとなり，不完全といえる．

パスワードの漏洩リスクをカバーする目的で，パスワードをICカードに格納する「スマートカード（ICカード）」の使用も認証技術として広く利用されている．ICカードはパスワード以外の電子情報を格納することが可能であることから，認証を含む多目的な用途での応用が可能である．しかしながら紛失リスク対応という観点でPINの併用が必須となり，セキュリティ強度の点で不完全といえる．

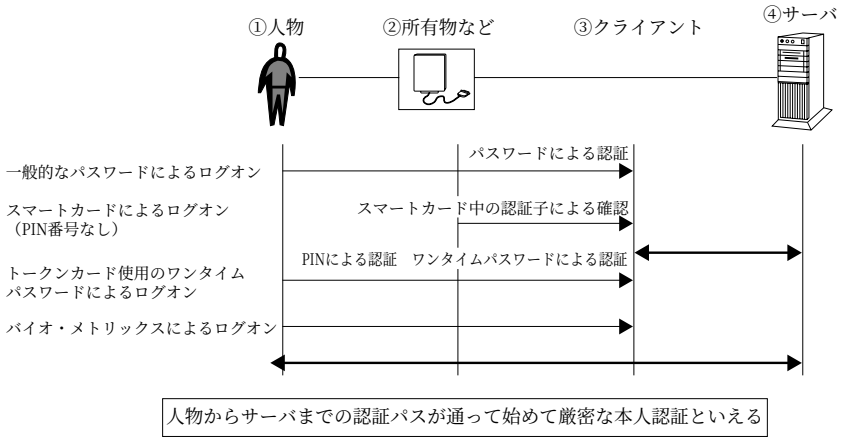
最近注目されているのは，バイオメトリックスを応用した「生体認証」と呼ばれる認証技術である．これは指紋，声紋，網膜パターンなどの生体的特徴による

認証が可能とした仮定に依拠した技術である．パスワードの漏洩リスク，パスワードトークンの紛失リスクの回避という点では全く問題がない．例えば指紋による認証では他人受け入れ率・本人拒否率といった精度の点で解決すべき課題はあるものの，総合的な認証強度の点では最も優れている．しかし，生体的特徴を使用することからプライバシの保全，すなわち第三者による管理が行われることに対する心理的な抵抗感の除去を先の精度の課題とあわせて解決する必要がある．

ネットワークシステム上で稼働する業務システムの普遍的な形態であるクライアントサーバシステムに「認証」手続きが存在する場所を図1に整理した．ここでは，

・人物と所有物などの間
・所有物などとクライアントの間
・クライアントとサーバの間

の各区間で認証手続きが存在し，各認証結果がすべてパスする，いわばリンクバイリンクでの認証パスが通ってはじめて厳格な認証手続きが行われたといえる，とする．



	なりすましの可能性					
	①－②	②－③	③－④	①－③	②－④	①－④
	人物－所有物	所有物－クライアント	クライアント－サーバ	人物－クライアント	所有物－サーバ	人物－サーバ
記憶認証	あり（予測等）	なし	あり（盗聴）	あり（予測等）	あり（盗聴）	あり（盗聴）
ワンタイムパスワード	×	なし	なし	×	なし	×
暗号技術利用(デジタル署名等)	×	なし	なし	×	なし	×
バイオ・メトリックス	なし	×	×	なし	×	×

図 1　認証パスの構造

「2.2節セキュリティ上の脅威と対策」の表1では，対応策として厳格なユーザ認証の必要を数ヶ所であげた．認証（とその手続き）における機構/機能の採用にあたってセキュリティ強度を高めるために重要な条件を以下に整理した．

・盗聴リスクの回避のために認証手続きにおける入力操作の排除

・ワンタイムパスワードトークン使用時の制約として知られる認証手続きの時間制限排除
・パスワードトークンの紛失リスクの回避
・生体的特徴の使用におけるプライバシ保護

これらの条件を満足するためには先の認証技術を複数種類組み合わせて使用することとなり，この結果対象となるネットワークシステム，業務システムごとに異なるユーザ認証のレベルに応じたセキュリティ対策の実現が可能となる．

クライアント―サーバ間の認証については次の「2）アクセス制御」のシングルサインオン機能で述べる．

2） アクセス制御

アクセス制御がネットワーク構成要素の全般にわたって提供する機能と実現するための技術を表3に整理した．

表 3　アクセス制御の機能と実現技術

機能	技術
厳格に行われたユーザ認証の結果に基いてユーザに必要なリソースを利用させる(＝必要なリソースしか利用させない)機構/機能	シングルサインオン
ユーザとユーザのセキュリティ権限に関する情報の登録/変更/削除を簡便にかつ一元的に実施する	
ユーザおよび管理者による情報へのアクセス履歴を監査する	ファイアウォール リモートアクセス
不正アクセス、使用不能攻撃を遮断する	
ネットワーク上流れるデータの盗聴と改竄が防止する	暗号化

① シングルサインオン

ユーザによる一回のネットワークシステムへのログオン操作（認証）でネットワーク上にあるすべてのアクセス権限のあるリソースを利用可能とする機構/機能である．データや業務アプリケーションの属性には依存しない特徴を持ち，先に述べた厳格なユーザ認証と併用することによって既存の認証（例えば，クライアント―サーバ間の認証）におけるセキュリティ強度を格段に高めることはもちろんのこと，管理者の運用負荷を軽減する．

ユーザにとっての利点には以下がある．

・サーバやアプリケーションにアクセスするごとにユーザ ID/パスワードを要求される煩雑さから解放される．

管理者にとっての利点には以下がある．

・ユーザ情報（セキュリティ権限などのプロパティ）の管理作業を大幅に効率化できる．
・パスワードなどユーザを認証するキーを統合し，それだけを集中的に管理すれば済むため，ネットワークシステム全体のセキュリティ強度が向上する．

シングルサインオンを利用することで実現できるセキュリティ対策の効果を図2に整理した．またシングルサインオン機能の構成例を図3に示す．

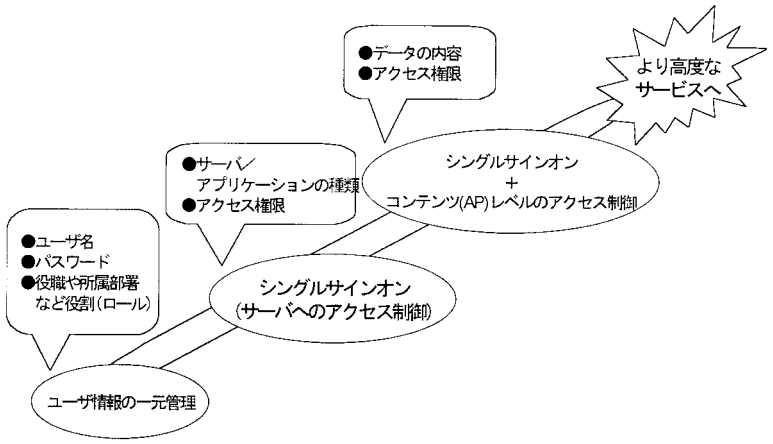


図 2　シングルサインオンによるセキュリティ対策とその効果

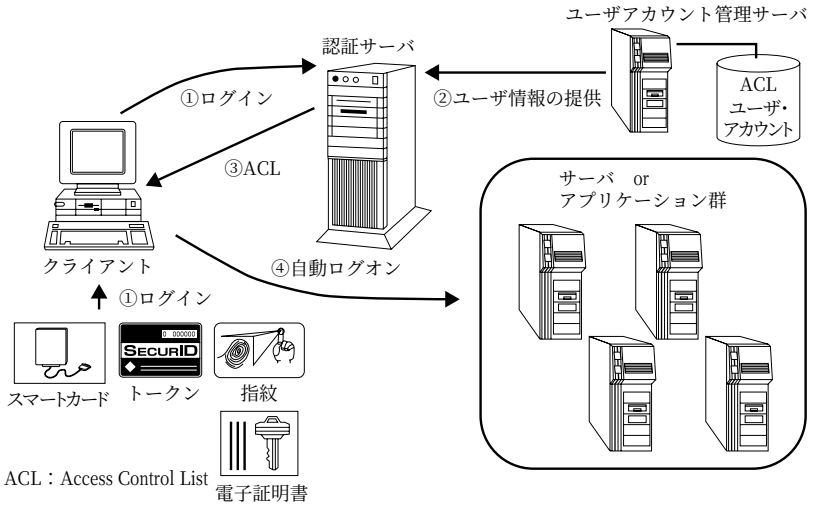


図 3　シングルサインオン機能の構成例

② ファイアウォール

ネットワークの表玄関ともいうべきファイアウォールは，外部，ことにインターネットとの接続において，外部からの不正アクセスを遮断する目的で非常に重要な技術要素である（図 4）．インターネットとの接続等に代表される外部ネットワークとの相互接続はネットワークの価値を格段に高めることができる．一方で外部からの不正アクセス，使用不能攻撃を受ける可能性は高く，万全のセキュリティ対策を施しておく必要がある．

ファイアウォール対策の要点は以下の通りである．

・必要なプロトコル種別，ポート番号のデータだけを通過させる設定をする．また不正アクセス，使用不能攻撃の疑いのある特定のインターネットアドレスを持つデータの遮断など，公知となったフィルタリングパターンを採

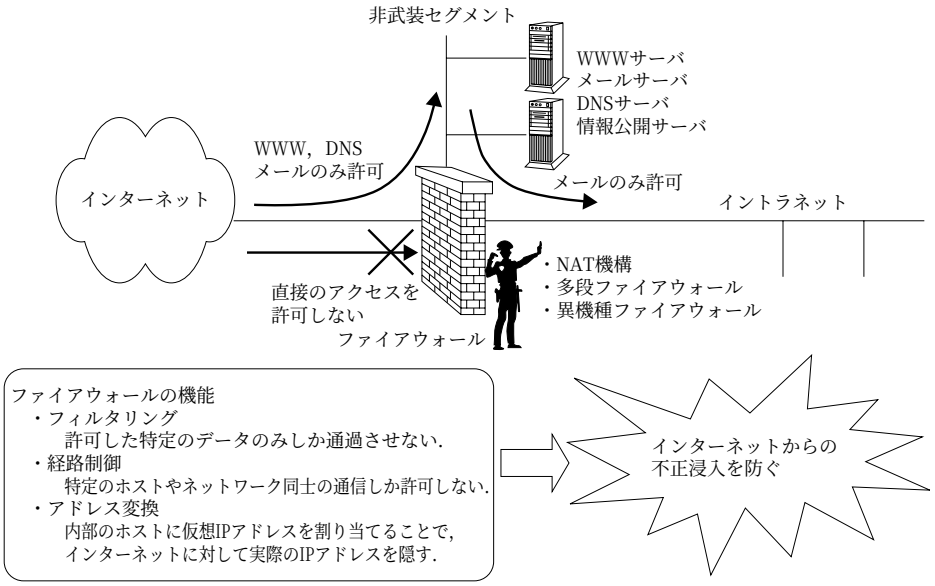


図 4　ファイアウォール

用する.

・複数のファイアウォールを設置してセキュリティ強度を高める.その場合,異なったベンダ製品または方式の異なるファイアウォールを採用し組み合わせる.

・NAT（Network Address Translator）機能によってネットワーク諸元（アドレス体系等）の秘匿を行うことも有効である.

・セキュリティ監視製品と連動して外部ネットワークとの接続を即時遮断するなどの処置も有効である.「3）状況監視/診断」で詳述する.

③　リモートアクセス

ネットワークの裏玄関ともいうべきリモートアクセスは，外部ネットワークとの接続という点ではファイアウォールと同じ位置づけにありながらセキュリティ対策が立ち遅れていることが多い（図 5）.

電話網に代表される公衆ネットワークの利用は，ネットワーク規模の拡大,ネットワーク利用者の範囲拡大といった点で有効な手段であるが，接続箇所の増加，ネットワーク利用者の不特定多数化という事態を招くこととなる.

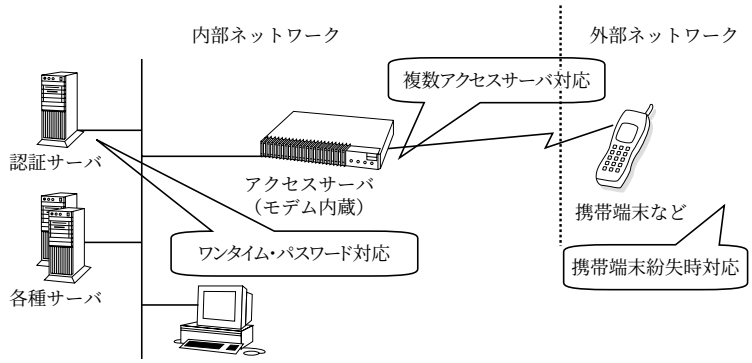
リモートアクセス対策の要点は以下のとおりである.

・特定利用者が利用する端末は，端末に格納された重要データの漏洩を防ぐための紛失リスクに対応する.

・公衆ネットワークを利用することによる盗聴リスクに対応する.

・公衆ネットワークとの接続においては，アクセスサーバと呼ばれる機器を使用することとなる．ネットワーク利用者の範囲拡大のためにはさまざまなアクセス方式/手段に対応可能にする.

・厳格な本人認証を行うために，ワンタイム性の高い（すなわちパスワード



□リモートアクセス環境
・アクセスサーバ
・ワンタイム性の高い認証機構の採用
・稼働管理
□データ暗号化
・ファイル暗号化ソフトウェアの導入
・紛失時対応

図 5　リモートアクセス

の漏洩リスク，パスワードトークンの紛失リスクを回避することができる）認証技術を使用したリモートアクセス認証機構/機能を採用する．

④　暗号化

暗号化技術は，セキュリティ対策の要素技術であるとともに，盗聴リスク回避のために重要ファイルやネットワーク上を流れるデータを暗号化するなど，セキュリティ対策の応用技術としても広く使用されている．アクセス制御の役割の一つであるデータの盗聴と改竄を防止する対策として具体的に以下のような機構/機能の使用を検討する．

・随時暗号/復号機能
特定のファイルまたはフォルダを会話形式で暗号/復号化する機能．
ネットワーク上を流れるデータの暗号化やクライアントの盗難リスクの回避などの対策として利用する．

・自動暗号/復号機能
指定したファイルまたはフォルダをクライアントログイン時に自動的に復号化し，ログアウト時に自動的に暗号化する機能．
クライアントの盗難リスク回避などの対策として利用する．
（暗号化技術については第 4 章参照のこと）

3）　状況監視/診断

セキュリティ対策における状況監視/診断技術は大きく以下の三つの技術要素に分類される．

・セキュリティ診断
・セキュリティ監視
・セキュリティ監査/認定

①　セキュリティ診断

外部からの不正アクセス防止という視点で定期的なネットワークシステムの診断を実施すべきである（図 6）.

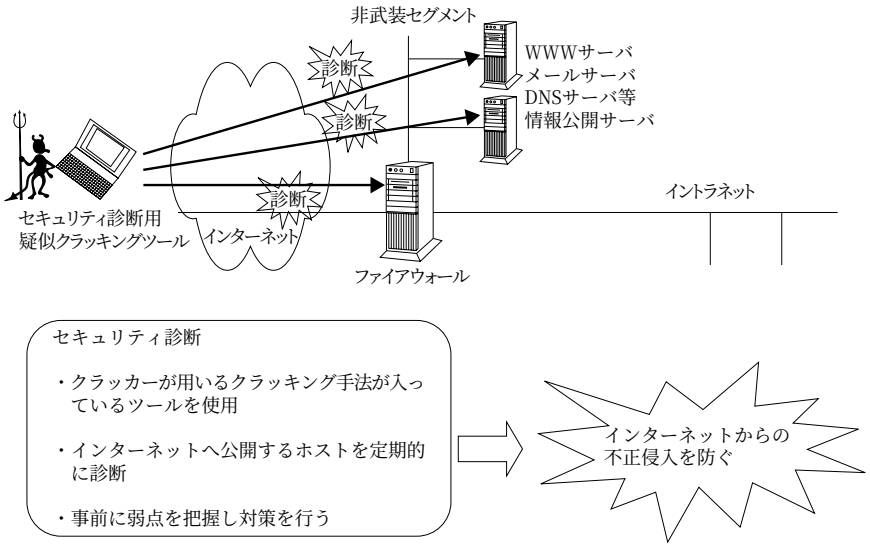


図 6　セキュリティ診断

セキュリティ診断対策の要点は以下の通りとなる.

・機構/機能の導入にあたっては，クラッカー（システムの破壊等を意図した悪意を持つハッカー）と同等レベルのクラッキングが可能であることを条件とする.

・定期的に，またはネットワークシステムの構成変更時にセキュリティ診断を実施する.

・診断結果を基に，セキュリティホールが確認された場合は速やかに対処を施す.

② セキュリティ監視

セキュリティ診断がネットワークシステムのセキュリティホールの診断を定期的に実施する対策であるのに対して，セキュリティ監視（図 7）は外部からの不正アクセス，使用不能攻撃等を検出し，不正行為による被害を最小限度にとどめる目的で使用される.

セキュリティ監視対策の要点は以下の通りとなる.

・ネットワークシステムの管理区画単位（ファイアウォール等で外部からの不正アクセス，使用不能攻撃等を防ぐ対応を図った区画単位)に導入する.

・24 時間，365 日の継続的な監視を実施する.

・不正アクセス，使用不能攻撃を検出した場合，直ちに当該区画の管理者への通報，ファイアウォール製品と連動して外部ネットワークとの接続の遮断といった処置を行う.

最近では，各クライアントにインストールするセキュリティ監視製品も提供

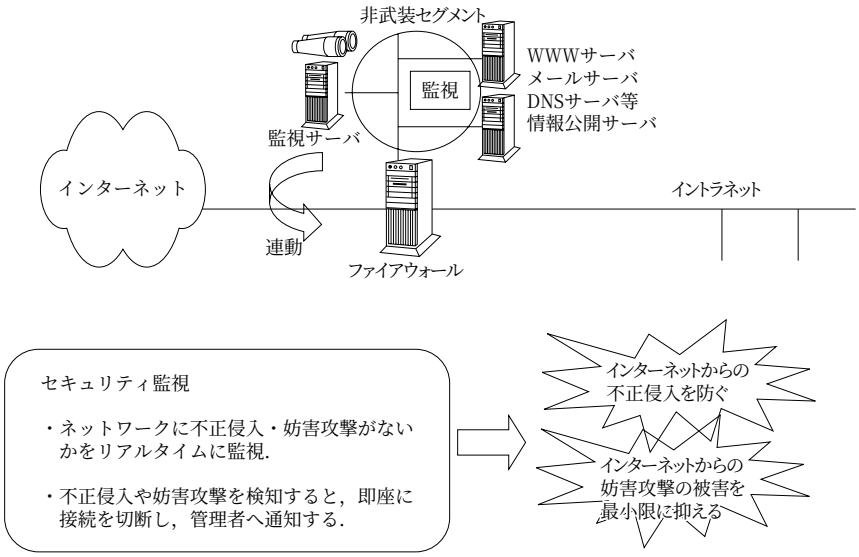


図 7　セキュリティ監視

されており，セキュリティ強度の向上のためには有効な手だてといえる.

③　セキュリティ監査

セキュリティ監査/認定とは，第三者がある監査/評価基準に基いて対象ネットワークシステムのセキュリティ強度を監査し，その結果を基に認定を行うことで，ネットワークシステムのセキュリティ対策レベルを客観的に評価し公開することが可能となる（図 8）. 利用者に対するネットワークシステムの信頼度を公開することはネットワーク利用者の範囲拡大のために有効な手だてといえる.

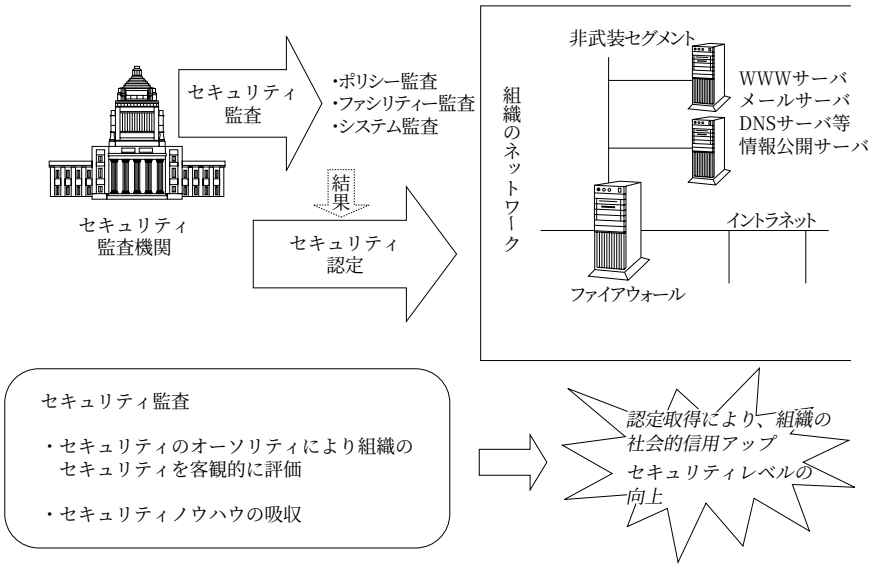


図 8　セキュリティ監査/認定

セキュリティ監査/認定対策の要点は以下の通りである．

・セキュリティ評価基準として ISO/IEC 15408 または 13335 などの国際標準への準拠性または BS 7799（英国標準）への準拠性を採用選定の基準とする．ただし，現在商用デファクト標準ともいえるベンダ，製品の採用選定も現実的な解といえる．

・定期的なセキュリティ診断の実施を併用し，セキュリティ強度維持を継続的に保守する．

4） ウィルス対策

ウィルス対策は，ファイアウォール，SMTP/POP メールサーバ，Web サーバなどのゲートウェイやアプリケーション/ネットワークサーバおよび全クライアントでウィルス対策ソフトウェアを使用して，はじめてネットワークシステムとしての対処が可能といえる（図 9）．

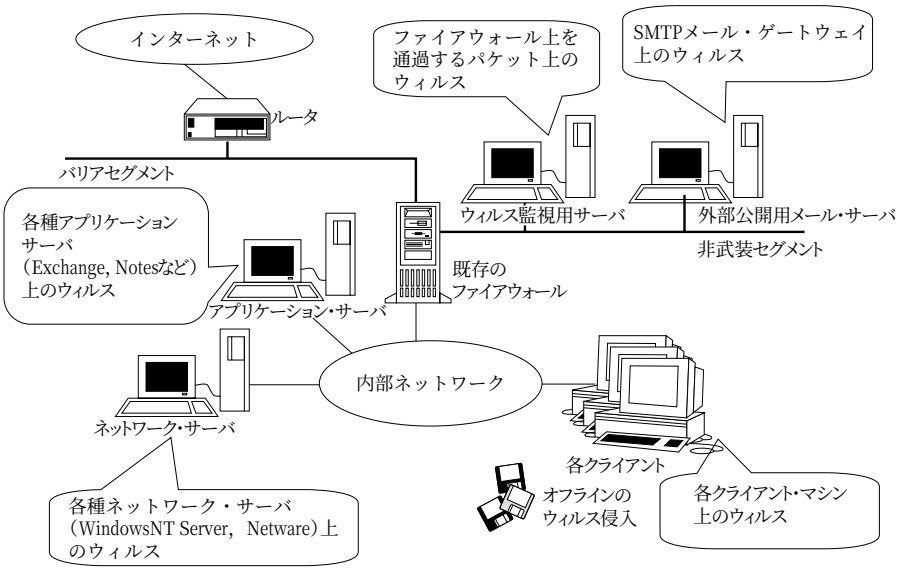


図 9　ウィルス対策

ウィルス対策の要点は以下の通りとなる．

・常駐させる

定期的にウィルスチェックを実施するだけでなく，常駐させることで操作対象となる全メディア，電子メール，Web ブラウザによるファイルのダウンロードなどに即応する．

・常に最新のウィルスパターンファイルを使用する

ウィルスパターンファイルにウィルスのパターンが存在しないとウィルス対策ソフトウェアの機能を果たせない．

・集中管理を行う

ネットワークに接続されたすべての機器にウィルス対策を施す．またウィルスパターンファイルの更新も同時に行われないとウィルス対策の効果も半減

する．組織としての対応を含み，ワクチンファイルを集中管理する．

3. 情報セキュリティ管理

3.1 組 織 体 制

組織の情報セキュリティを実現するためには，情報セキュリティ関連施策をトップダウンで管理・運営する体制が必要である（図 10）．

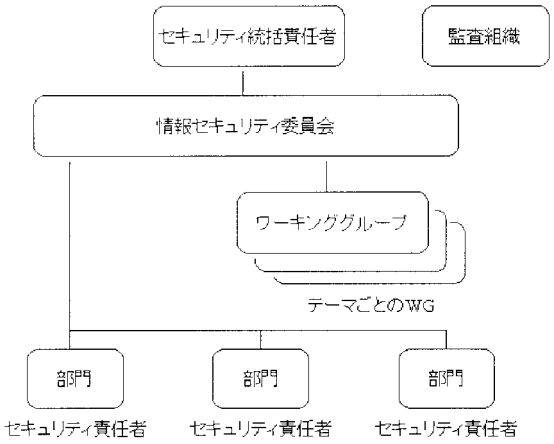


図 10　情報セキュリティ管理運営組織の例

① 情報セキュリティ統括責任者

組織内のすべての情報セキュリティに関して中心となって活動して意思決定を行う．主な責任・役割は以下である．

・情報セキュリティ委員会を開催する．

・情報セキュリティ委員会の協議に基づいてセキュリティポリシーの制定・改訂などの情報セキュリティ関連施策を承認する．

② 情報セキュリティ委員会

組織の多分野にわたる情報セキュリティ関連施策を協議したり問題に対する具体策を立案し組織内に通達・徹底するためのオーソライズの場である．情報セキュリティと技術面に背景知識をもつメンバと，情報システムの提供者およびユーザの代表者とを含めるのが望ましい．

主な責任・役割は以下である．

・情報セキュリティ関連施策を協議する．

・情報セキュリティ関連施策の普及・維持を統括・監視する．

・各部門(プロジェクト，システムなど)のセキュリティ責任者を任命する．

③ ワーキンググループ

テーマごとに関連する組織の責任者，実務担当者と有識者が集まり，具体的な情報セキュリティ関連施策を検討し，立案する．

主な責任と役割は以下である．

・テーマごとに情報セキュリティ関連施策を検討し，草案を作成する．

・情報セキュリティ委員会に提案する．

④ 監 査 組 織

組織内の状況が情報セキュリティポリシーなどに準拠しているか，情報セキュリティポリシーが妥当であるかなどを定期的に監査する．

主な責任・役割は以下である．

・組織内の状況が情報セキュリティポリシーなどに準拠しているか，情報セキュリティポリシーが妥当であるかなどを監査する．

・情報セキュリティ統括責任者と情報セキュリティ委員会へ監査結果を報告する．

⑤ セキュリティ責任者

各部門ごとに設置される．情報セキュリティ関連施策の周知徹底させ，監督指導を行う．

主な責任と役割は以下である．

・セキュリティポリシー，情報セキュリティ関連施策を周知徹底させ，監督指導を行う．

・情報セキュリティ委員会へ状況を報告する．

3.2 セキュリティポリシー

組織の情報セキュリティの考え方であるセキュリティポリシーは保護すべき対象範囲と対策手段および管理運営方法についての方針を記した文書である．セキュリティポリシーに基づいて具体的な運用管理規程を定める．セキュリティポリシーを策定する際には，セキュリティ管理の考え方や手法についてのガイドラインを記した ISO/IEC 13335（GMITS）やリスク分析・各種管理基準などの具体的な要件集である BS 7799 などの国際的な標準を活用する（GMITS，BS 7799 については第 4 章を参照のこと）．

4. 情報セキュリティ技術に関する標準化動向

データの機密性の保護と認証を実現するメカニズムとして利用される暗号技術は情報セキュリティの中核技術であり，システム設計や開発においては技術の前提となる暗号アルゴリズムなどの技術標準も必要となっている．

情報処理製品や情報処理システムの開発・製造・運用に関わった資材を検査してどの程度保証されているかを確認するための国際的な評価基準として ISO/IEC 15408（JISX 5070）がある．

組織体の事業を継続ならしめるために情報セキュリティ対策活動がマネジメント活動に組み込まれ，他の組織との取引などにおいて信頼を寄せる基礎となっており，その確保が必須となっている．このような現状において，とくにインターネット上などでの国境のない取引でその実践規範ないしはガイドラインが国際的に共通理解できることが求められており，ISO/IEC 13335（GMITS）や BS 7799 が注目を集めている．

4.1 暗 号 技 術

暗号化方式は鍵の用法によって二つに分類される．

1） 秘密鍵暗号方式

暗号化と復号化で同じ秘密共通鍵を使用する．暗号化/復号化のスピードが速く，主としてデータの暗号化に用いる．

暗号化通信を行う場合，データの送信者と受信者間で暗号化/復号化に必要な同じ秘密共通鍵を保有するために，秘密共通鍵を両者に安全に配送，管理するしくみとして鍵管理（Key Management）が重要となる．暗号化通信する相手ごとに秘密共通鍵をもたなければならないため，鍵の数が膨大になる．代表的なアルゴリズムにはDES（Data Encryption Standard：米国政府の標準暗号化方式FIPS 46[*1]），Triple-DESなどがある．56ビット鍵長のDESは暗号としての寿命がきているため，NIST[*2]により次世代の米国標準暗号アルゴリズム（AES）の選定作業が行われ2000年10月にRijndaelが選ばれた．AESは128ビットから256ビットの鍵長をもつ．量子コンピュータなど新しい技術による超高速コンピュータが現れないかぎり，現状の技術によるコンピュータのマシンパワーの急激な向上を考慮しても21世紀中は解読されることはないといわれている．

2） 公開鍵暗号方式

公開鍵暗号方式は暗号化と復号化で違う鍵を使用する．一組の鍵のうち，一方の鍵を公開（公開鍵）し，もう一方の鍵を秘密（秘密鍵）とする．公開鍵で暗号化し，秘密鍵で復号化する．主として認証に用いる．暗号化通信を行う場合，相手の公開鍵を取得して暗号化すればよいため，秘密鍵暗号方式とくらべて，送受信者間で秘密の情報を交換する必要がない，鍵の数が少なくて済むという利点がある一方，暗号化に時間がかかる欠点もある．

主な公開鍵暗号アルゴリズムには以下がある．

・RSA

十分に大きな素数の積を素因数分解することが困難であることを利用している．公開鍵で暗号化，秘密鍵で復号化ができるだけでなく，秘密鍵で暗号化，公開鍵で復号化ができるため，前者は機密保護のための暗号化，後者は電子署名に利用される．デファクトスタンダード的な暗号アルゴリズムである．

・ElGamal

T. ElGamalによって開発された．離散対数問題の困難さを利用している．公開鍵と秘密鍵を逆に利用することはできない．DSA署名アルゴリズムの基礎となったアルゴリズム．

・ECC

楕円曲線上の離散対数問題の困難さを利用した楕円暗号アルゴリズム．RSAに比べて同じ安全性を短い鍵長で確保できる．ECCの160ビット鍵長がRSAの1024ビット鍵長相当する強度をもつ．

3） 標準化動向

情報処理製品やシステムのセキュリティ確保にはシステム設計・開発における技術の前提となる暗号アルゴリズム等の技術標準も必要である．ISO/IEC JTC 1では2002年にむけた標準暗号を検討中である．総論，公開鍵，共通鍵ブロック暗号，共通鍵ストリーム暗号の4パートがある．日本の企業も公開鍵と共通鍵ブロック暗号のパートに候補を出している．

日本では2003年を目途としてその基盤を構築することとしている電子政府において，セキュリティの共通基盤の確保が重要な課題となっている．電子政府における適切な暗号利用をはかるため，政府の利用方針を策定する必要性が指摘されている状況において，政府は情報処理振興事業協会（IPA）を事務局とする暗号技術評価委員会（CRYPTREC：Cryptography Research and Evaluation Committee）を設置した．CRYPTRECは適用される暗号技術のリストアップ，専門的・客観的見地からの評価，調査，利用可能技術の特徴を調査する．対象は公開鍵暗号，共通鍵暗号，ハッシュ関数，疑似乱数である．

4.2 ISO/IEC 15408

欧米の政府機関が導入する情報処理製品やシステムの調達基準として開発された評価基準CC（Common Criteria）をもとに国際規格化されたものである．

情報処理製品やシステムを導入するユーザ機関が製造者に対して要求するセキュリティ機能の機能要件と保証要件を定めている．機能面は利用者本人の確認方法やデータの不正利用からの防止方法といったセキュリティ機能に関する技術的対策が中心であり，保証（品質）面はセキュリティメカニズムが有効に動作するための保証や機能が正しく実装されているかどうかの検証が中心となっている．検査対象となる資材としては，プログラム設計書，プログラムソースコード，オブジェクトコード，テストドキュメント，マニュアル，教育・業務規約などといった通常の開発や運用で作成するものと，ISO/IEC 15408特有のセキュリティ基本設計書（ST：Security　Target）と脆弱性分析書などがある．保証レベル（保証要件の尺度）は技術的なセキュリティ強度を保証するものではなく，セキュリティ検証をどの程度深くおこなうのかを定義したものである．

情報処理製品やシステムがISO/IEC 15408に準拠して製造されたことを第三者が検査・評価して認証する制度としてセキュリティ評価・認証制度が運用されている．ISO/IEC 15408の評価・認証制度は国際的な相互認証協定が結ばれており，参加各国間では認証を受けた製品やシステムは他国でもその認証が有効となる．相互認証協定にはカナダ，フランス，ドイツ，イギリス，アメリカ，オーストラリア，ニュージーランドをはじめとする国々が参加している．日本政府は2001年から評価・認証体制を創設し運営を開始する計画を進めており，日本の相互認証協定への参加は2003年を目指すとしている．

4.3 セキュリティマネジメント標準規格

ISO/IEC 15408は情報処理製品やシステムの製造工程におけるセキュリティ対策に着目した評価であり，その製品やシステムを運用管理するうえでの組織の管理体制は対象となっていない．人間系のセキュリティマネジメントを中心に規定した標準にはBS 7799やISO/IEC 13335（GMITS）があり，国際的な標準規格として利用されている[2]．

1） BS 7799

情報セキュリティ管理を規定した英国標準（BS）である．欧州を中心に世界各国で準拠あるいは参考にされており，事実上の標準といえる．英国主導で国際的な認証制度c：cureが確立されている．

以下の 2 パートから構成されている．

・Part 1　情報セキュリティ管理基実施基準（DIS 17799–1）

Part 2 の要求事項をサポートするベストプラクティスについての手引き書．リスク分析，具体的な運用などの実践的な規範となるセキュリティマネジメント手法を提供するものである．

・Part 2　情報セキュリティ管理システム仕様

情報セキュリティ管理システム（ISMS）の確立，実行および文書化についての要求事項が規定されている．また個々の組織の必要性に応じたセキュリティ管理策についての要求事項を規定している．Part 2 の第 4 章に記述される管理目的および管理策は Part 1 から直接引用されている．評価・認証の基礎となる．

2)　ISO/IEC 13335（GMITS）

情報処理製品やシステムを導入したユーザにおいてシステムの運用に関わる管理手続き等に関する指針を定めている．セキュリティマネジメントの概念的なフレームワークを提供するものでトップダウン的なアプローチをとる．以下の 5 パートから構成されている．

・Part 1　情報セキュリティのための概念とモデル
・Part 2　情報セキュリティのマネジメントと計画
・Part 3　情報セキュリティのマネジメント技術
・Part 4　セーフガードの選択
・Part 5　ネットワークセキュリティ上のマネジメントガイダンス

日本では 2000 年 12 月完成予定をめざして JIS 化作業中である．

5. おわりに

具体的なセキュリティポリシーやガイドラインを策定するために，前提となる検討項目や技術要素, さらにはセキュリティ確保のための基本的な考え方を解説してきた．当然のことながらただ技術的強度さえ高めればセキュリティ強度が高まるわけではない．すなわちどんなに高度な技術を援用したところでこれを利用する人間が適切な対応をしなければセキュリティは無きに等しい．技術とマネージメントはセキュリティの両輪であり，総合的なセキュリティ対策が必要である．

各種の情報セキュリティ標準の国際規格はグローバルなビジネス展開において取引相手企業のセキュリティ適正を確認する手段として用いられるようになり，ビジネスに多大な影響を与えることになるであろう．

[付録] 認証技術

認証技術は大別して二つの要素から構成される．

・Authentication

エンティティに対する真正性を証明する技術，すなわちあるエンティティが別のエンティティに対して，真正であることを証明する方法または同一性を証明すること

・Certification

エンティティに対する真正性を伝達する技術，すなわちあるエンティティが別のエンティティに対して，真正であることを証明した例証（インスタンス）またはその手続き

システムをめぐる認証技術は当該システムに関与するすべての実体（エンティティ：人間，プロセス，ソフトウェア，ハードウェアなど）に対して存在する．ここでは上記の認証技術のうち，Authentication，すなわちエンティティに対する真正性に関する技術を解説する[*3]．

1） エンティティ認証技術

情報通信において必須とされるエンティティ認証とは，情報通信に関与したエンティティが正当なものであるか否かを確認することである．既存の各方式は種々問題を抱えており，インターネット時代においてはこれら問題を解決し，かつその適用領域の広範さと相互接続性の観点から，導入・仕組みが簡単で，さらに様々な脅威に対して十分有効な方式が望まれる．エンティティ認証技術は認証に使う情報のあり方によって次の四つに分類できる．

・知識利用
・暗号利用
・生体特徴利用
・所有物利用

2） 知識利用によるエンティティ認証技術

本人だけが知る情報（ログイン時のパスワード，ATM での銀行預金引き出し時の暗証番号など）を使用する．導入が比較的簡単であるが，推測されやすいパスワードを使用したり，通信中に盗聴されるなどのリスクがある．たとえパスワードを送信する時に暗号化しても毎回同じパスワードであれば再利用される可能性がある．また，サーバのパスワードファイルが暗号化されていても辞書攻撃などで破られる可能性もある．

これらの脅威に対抗するために一回だけ使用できる使い捨てのワンタイムパスワードが考案されている．パスワードが毎回異なるため，盗んだパスワードを再使用すること（リプレイ攻撃）を防ぐ．

ⓐ ワンタイムパスワード方式

Bellcore Co. U.S.A. が提唱した S/Key（RFC-1938）が有名である．

処理概要（A：クライアント，B：認証サーバとする）は以下のとおり．

① 一方向性関数 f を準備する．

② A は秘密の乱数 R と公開の種と呼ばれる任意の数値 S を生成する．

③ Q＝R＋S とし，f(Q)，f(f(Q))，f(f(f(Q)))，…を計算し，それらを X_1，X_2，X_3，X_{100}，X_{101} とする．

④ A は X_1，…X_{100} および R を秘密に保持し，B には X_{101} を何らかの方法（オフライン）で渡す．B は X_{101} を保持する．

⑤ A が B に初めてログインする際，パスワードとして X_{100} を B に送信する．

⑥ B は f(X_{100}）を計算し，保持していた X_{101} と比べる．一致すればログインを許可し，一致しなければログインを拒否する．ログインが許可された場合，B は X_{101} を捨て，X_{100} を保持する．

⑦　A が次にログインするときは X_{99} を使用する．B の処理は以降同様である．

長所には，

・一回限りのパスワードなので，通信中で盗聴されても再利用できない．

・サーバにあるパスワードは次回のパスワードを検証するためのものなので，盗まれても問題ない．

・関数 f は一方向性関数なので，Xn が盗聴できても Xn−1 が計算できない．従って，第三者が f を知っても問題ない．

などがある．

短所には，

・準備したパスワードを全部使いきると，サーバの認証プログラムを再初期化する必要がある．

・実際にはオンラインで再初期化できるように実装されている．サーバは常に乱数 R を保持しており，クライアントは前回とは異なる種 S ’だけをサーバに送信し，サーバは Q ’＝R＋S ’を計算し，新たな X ’101 を生成する．第三者がサーバに不正侵入したり，悪意あるサーバ管理者が R を得ると，クライアントになりすますことができる．

などがある．

ⓑ　チャレンジレスポンス方式

代表的なものに CHAP（Challenge Authentication Protocol，RFC−1334）方式がある．最初に認証を行うサーバ側からチャレンジ（C）と呼ばれる何らかの毎回異なる情報が認証をうけるクライアント側に送られる．クライアント側ではシークレット（S）と合わせて R＝f(C，S）を計算して，その結果をレスポンス（R）としてサーバに送り返す．シークレットはサーバとクライアントで共通に持つ情報で，f は定まった関数なので，サーバ側でも同じ計算をして送られてきた R と比較することができる．両者が一致すればクライアントがシークレット（S）を正しく知っていることが確認できる．チャレンジ（C）が毎回異るためレスポンス（R）も毎回変わる，シークレット（S）はネットワーク上をやり取りされない，関数 f はハッシュ関数などの一方向性関数なので C と R を知っても S を逆演算で求めることはできない，などが特徴である（図 11）．

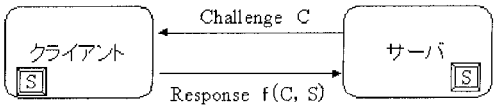


図 11　チャレンジレスポンス方式

長所は，チャレンジが毎回変化するので，第三者がメッセージを盗聴しても再利用が不可能なことである．

短所は，サーバ上にクライアントのパスワードが保存されているので，サーバ管理者がクライアントになりすませることである．

3）　暗号利用によるエンティティ認証技術

暗号技術を用いて当事者以外には偽造が困難な認証情報を生成し，当事者間で交換し，検証する．

ⓐ　電子署名

公開鍵暗号方式を利用してなりすまし，改ざん，否認を防止する機能を提供する．データに改ざんが加えられていないことを保証し，かつ，そのデータを作成したエンティティが確かにそのエンティティそのものであることを保証するメカニズムである．

ネットワーク上でのメッセージの送受信では，送信者はメッセージをハッシュ関数で圧縮して生成したメッセージダイジェストを公開鍵暗号方式で送信者の秘密鍵を使って暗号化し，これを電子署名としてメッセージに添付して送信する．受信者は，メッセージをハッシュ関数で圧縮してメッセージダイジェストを得，次に添付された署名を送信者の公開鍵で復号化し，メッセージダイジェストとこれを比較する．署名は本人しか知り得ない秘密鍵で作成されているため送信者以外には偽造できず，公開鍵で署名の検証をおこなったときには，相手の認証ができるだけでなく，送信したことを否認できないことになる（図 12）．

ハッシュ関数とは，任意長のメッセージを固定長に圧縮する関数で，同じ圧縮結果が得られる二つの元のデータを見つけることが困難であること（衝突をおこしにくい），ある特定の圧縮結果を抽出できるような元データを見つけることが困難であること（圧縮結果から元データを見つけられない）の二つの性質を持つ．代表的なハッシュ関数には，MD 2，MD 5，SHA−1（FIPS 180−1）がある．

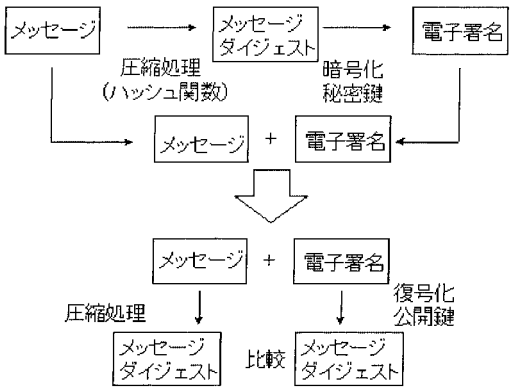


図 12　電子署名のしくみ

主な電子署名アルゴリズムの種類には以下がある．

・RSA

RSA 暗号アルゴリズムを利用している．一般には 512，1024 ビット程度の鍵長が用いられている．ハッシュ関数には MD 2，MD 5，SHA−1 を使用．もっとも広く使われてデファクトスタンダードとなっている．

・DSA

ElGamal 暗号アルゴリズムを利用している．1994 年に NIST の電子署名標準

（FIPS 186 DSS）として採用された．鍵長は 1024 ビットが用いられている．ハッシュ関数には SHA-1 を使用．政府系標準として多くの製品で採用されている．

・ECDSA

ECC 暗号アルゴリズムを利用して DSA と同じ手順で署名を行う方式．RSA や DSA に比べて同じ安全性を短い鍵長で確保できる．ECC の 160 ビット鍵長が RSA の 1024 ビット鍵長に相当する強度をもつ．FIPS 186-2 として NIST の標準となっている．IC カードなど処理能力の小さい CPU 上で採用されはじめている．

電子署名を用いて受信者が送信者の正当性を確認するには，送信者と公開鍵の結びつきの保証が必要である．認証機関（CA： Certification Authority）は公開鍵とその持ち主の関係を保証する証明書を発行する．公開鍵暗号方式による電子署名と認証機関および認証機関が発行した証明書を利用する認証方式については「(6) PKI による認証」で述べる．

公開鍵暗号方式による電子署名では署名用の秘密鍵を厳密に管理することが必要となり，秘密鍵の格納先として IC カードの利用が広まっている．

ⓑ SSH（Secure Shell）

リモートログインやリモートコマンドのセキュリティを強化するプログラムである．rlogin，rcp や rsh の代わりに使用し，認証機構の改善や通信内容の暗号化などにより安全な通信環境を実現する．基本的には秘密鍵暗号と公開鍵暗号を併用したチャレンジレスポンス方式である．

図 13 に認証処理に関する概要（A：クライアント，B：サーバとする）を示す．秘密鍵暗号のセッション鍵を共有するフェーズ（②，③）と認証処理を行うフェーズ（④，⑤，⑥）がある．

① A は B にログイン要求を送る．

② B はセッション鍵共有のため自分の公開鍵，乱数などを A に送る．

③ A はセッション鍵を生成し，B の公開鍵で暗号化して B に送る．B がこれを受信した時点で A との間にセッション鍵を共有できたことになる．④以降は AB 間のメッセージは全てこのセッション鍵で暗号化される．

④ A は，自分の公開鍵，ユーザ名を B に送る．

⑤ B は A に対する公開鍵とユーザ名が登録されていることを確認の上，認証のためのチャレンジ（乱数）を生成し，A の公開鍵で暗号化して A に送る．

⑥ A はチャレンジのハッシュ値を計算し，レスポンスとして B に送る．

⑦ B は，⑥で受けたレスポンスの値と保存してあった A 用チャレンジのハッシュ値を比較し，同じであれば A のログインを許可し，異なっていればログインを拒否する．

長所は，チャレンジデータが毎回変化するので認証情報を盗聴されてもなりすましは不可能なことである．

短所は，サーバの管理者が悪意でクライアントの公開鍵情報を書きかえることによりクライアントになりすますことが可能なことである．

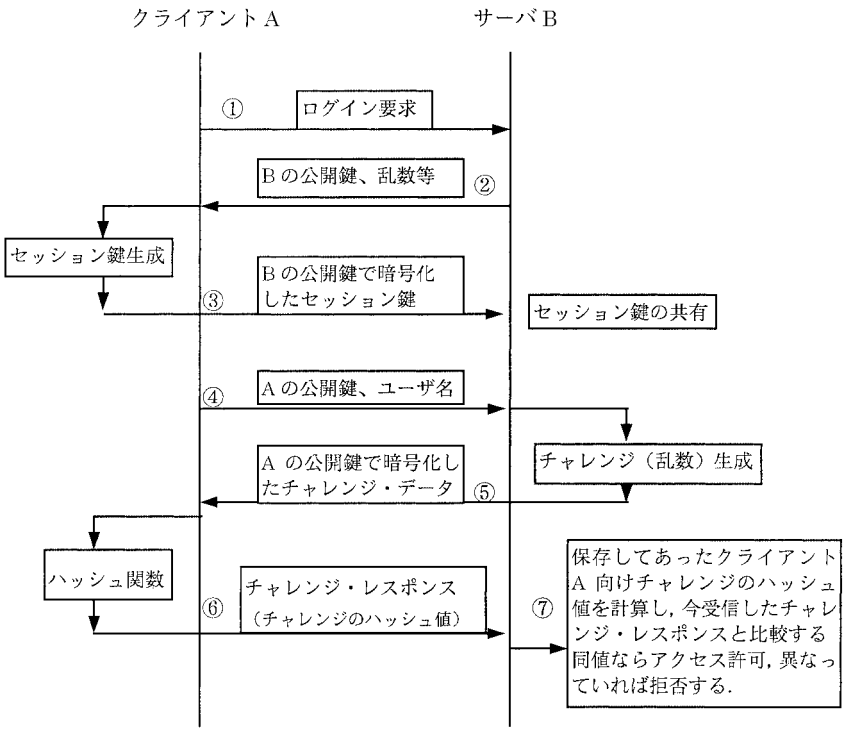


図 13　SSH の概要

ⓒ　RPC のエンティティ認証方式

UNIX の遠隔手続き呼び出し機能である RPC（Remote Procedure Call）には，セキュリティ機能としてユーザ認証機能がある．RPC 認証は，RPC 手続きの発行者が誰であるか，発行者の権限はどの程度かをサーバが確認する機能を備えている．図 14 に RPC のユーザ認証処理概要（A：クライアント，B：サーバとする）を示す．

①　A と B は DES 暗号に用いる共有鍵（Kab）を DH 法（Diffie-Hellman 型公開鍵配送法）により共有する．

UNIX では DH 法に用いる公開鍵と秘密鍵を NIS（Network Information Service）で管理している．各ユーザは通信に先立って NIS から通信相手の公開鍵と自分の秘密鍵を入手し，共有鍵（DES 鍵）を計算する．

②　A は以下の手順で認証情報を作成して B に送信する．

（Ⅰ）送信者を表す文字列（ネットネーム）を生成する．

（Ⅱ）セッション鍵（乱数：K）を生成する．

（Ⅲ）タイムスタンプ（現在時刻：T）をセッション鍵（K）で DES 暗号化する（Te）．

（Ⅳ）セッション鍵（K）を共有鍵（Kab）で DES 暗号化する（Ke）．

認証情報として，（Ⅰ）（Ⅲ）（Ⅳ）を B に送信する．

③　B は，受信した認証情報の中の暗号化されたタイムスタンプ（Te）を復号化し（T），現在時刻と比較してネットネームの正当性を検証する．T と現在時刻との差が許容範囲内であればそのネットワークのアクセス要求を許可するが，許容範

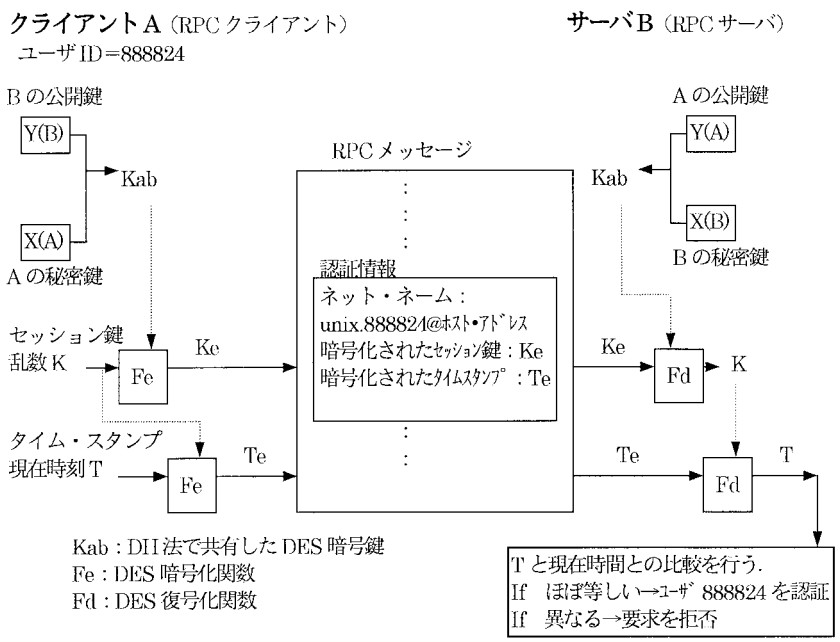


図 14　RPC認証の概要

囲外であれば拒否する.

長所には,

・クライアントとサーバが自分の秘密鍵を厳密に保持し，かつ正当な相手の公開鍵を確実に得ることができればなりすましは困難である.

などがある.

短所には,

・一定時間内であれば，盗聴などにより認証情報を再利用される可能性がある.

・サーバ管理者はクライアントの認証情報を作成できるので，クライアントになりすますことができる.

などがある.

ⓓ　Kerberos（RFC-1510）方式

Kerberosは「信頼された第三者機関による認証方式」に基づく利用者認証システムである．MITのAthenaプロジェクトで開発された．OSF[*4]が定めた分散処理環境構築システムDCE（Distributed Computing Environment）で採用された.

ユーザ側のシステムにユーザのパスワードや鍵が長時間存在しないように認証サーバ（AS：Authentication Server）と鍵配布サーバ（TGS：Ticket Granting Server）の二つのサーバによって認証が行なわれること，通信の秘匿やユーザー認証などをすべて秘密鍵暗号方式（DES）で実現していることが特徴である（図15）.

長所には,

・各サーバ，クライアント間のやりとりは全て暗号化され，さらに暗号化鍵は毎回乱数から生成するので盗聴に強い.

・目的サーバは各ユーザのユーザIDやパスワードを管理する必要は無く，Kerberos

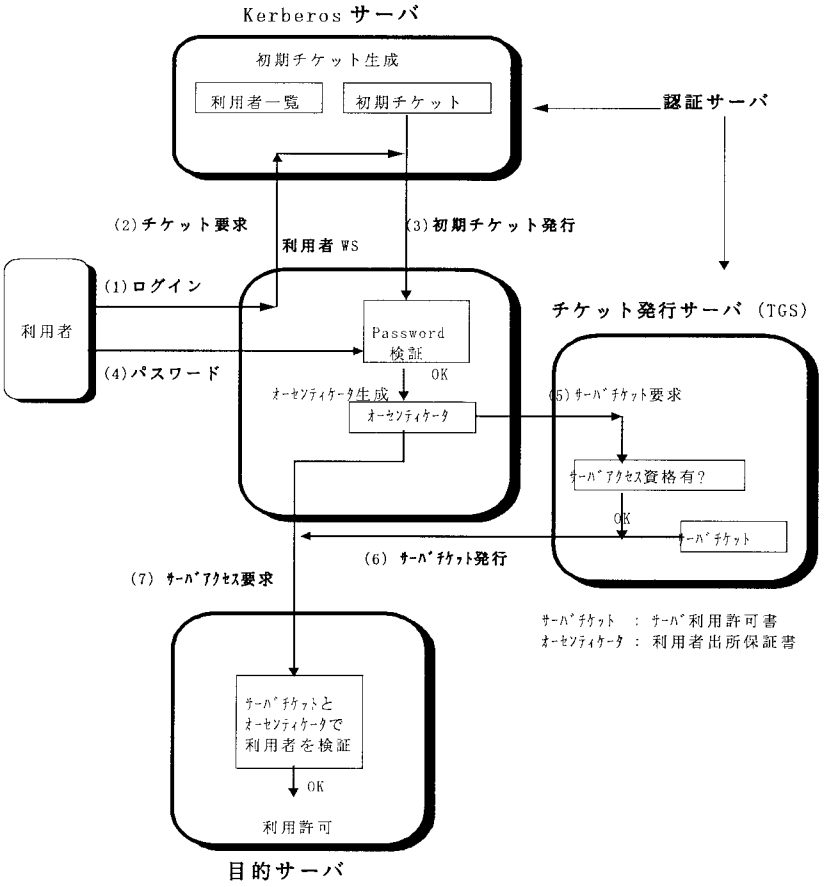


図 15　Kerberos 認証方式の概要

サーバだけが知っていればよい．このため大規模分散環境における変更管理が容易になる．

などがある．

短所には，

・一定時間内であれば盗聴した認証情報を再利用できる．

・認証サーバが各ユーザの認証情報や暗号化鍵を集中管理するので，悪意の第三者が認証サーバに侵入するとその管理対称ドメインが全滅する．

・全てのマシン，アプリケーションに Kerberos 対応が必要なので，導入の手間が大きい．

などがある．

仕様ではベンダ固有のフィールドを定義できるので，Kerberos 準拠の製品であるとはいってもベンダ間で相互運用性があるとは限らないことに注意する．たとえば最近 Windows 2000 で Kerberos が実装されたが，ユーザ認証にログオン名でなく SID（Security IDentifier）などの情報を利用しており，UNIX など他の Kerberos システムが発行したチケットを Windows 2000 で認証することはできない．

ⓔ　ゼロ知識対話証明方式

自分がある情報を知っているときに，相手にその情報を教えることなく自分がその情報を知っていることだけを証明する方式である．MIT の Goldwasser，Micali とトロント大学の Rackoff が提案した．パスワードを提示せずに真のパスワードを知っていることを相手に証明することができる．クライアント A がサーバ B へ秘密情報 T を転送する場合の処理概要を図 16 に示す．

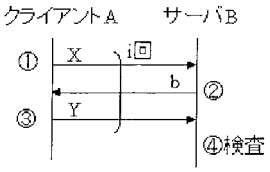


図 16　ゼロ知識対話証明方式の概要

A は $Z=T^2 \bmod n$ を完全に知り，B は Z と n だけを知っている．n は大きな素数 p，q の合成数であり，B は n を素因数分解できなければ T を得ることは困難である．

以下の①から④を i 回繰り返して A の正当性を検証する．

①　A は乱数 R を選び，$X=R^2 \bmod n$ を計算し，X を B に送る．

②　B は $b \in \{0, 1\}$ を二者択一的にランダムに選び，b を A に送る．

③　A は次の Y を B に送る．

$$Y=\begin{cases} R & b=0 \text{ の場合} \\ TR \bmod n & b=1 \text{ の場合} \end{cases}$$

④　B は次式が成立するかを検査する．

$X=Y^2 \bmod n$　b＝0 の場合

$ZX=Y^2 \bmod n$　b＝1 の場合

これらが成り立てば検査 OK とする．

（注 1）③，④で b＝0 と b＝1 の場合に分けるのは，A になりすました悪意のクライアント A ’は T の値を知らなくても以下のようにして検査に合格できるからである．常に b＝1 であるなら，A は①で Y の値として適当な Y ’を定め，X＝(Y ’)^2/Z mod n を計算し，X を B に送る．次に③で Y＝Y ’の値を送ると④の検査は当然合格する．

（注 2）b の値を予想してから検査式を満たす X と Y を計算できるので一回当たりのなりすまし確率は 1/2 である．従ってこの手順を i 回繰り返すとなりすましの確率を 2^{-i} にできる．

長所は事前に秘密の認証情報 T をサーバに教える必要がないので，サーバの正当な管理者であってもクライアントになりすますことができないことである．

短所は対話シーケンスが冗長であること，認証プロセスが複雑であるためパフォーマンスと認証精度がトレードオフの関係となることである．

ⓕ　無限ワンタイムパスワード

公開鍵暗号化方式を利用して一回限り有効な認証情報を無限に生成できる認証方式である．日本ユニシス株式会社八津川によって考案された．クライアントXとサーバY間の認証処理概要を図17に示す．

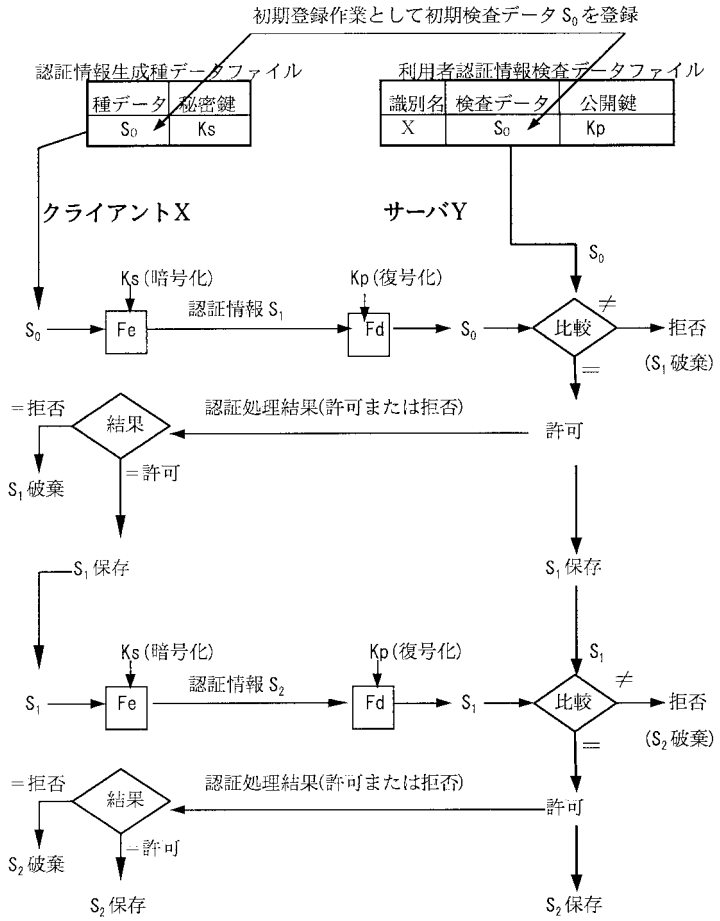


図 17　無限ワンタイムパスワードの処理概要

CKp　：CAによって発行されたクライアントXの公開鍵証明書
Ks　：Xの秘密鍵
Kp　：Xの公開鍵
Se　：公開鍵暗号アルゴリズムの暗号化関数
Sd　：公開鍵暗号アルゴリズムの復号化関数
Dn　：n回目のログイン時においてXがYに送信する認証情報
Dn−1：n回目ログイン時のXにおける認証情報生成種データ，Yおける認証情報検査データ

（注1）D0：初期登録値
Dn : Dn−1をKsで暗号化したもの（ただし，∞>n>1）である．

（注2）毎回，認証情報と共にXの公開鍵証明書をYに送るシステムであれば，利

用者認証情報検査データファイルに Kp および CKp を保存する必要はない．

① X はログイン時に利用者識別名（User-id など）を Y に送信して認証要求を行う．

② 認証要求を受けた Y は，X に対して認証情報要求メッセージを送る．

③ 認証情報要求メッセージを受け取った X は，保存している認証情報生成種データを秘密鍵で暗号化し，認証情報として Y に送る．一回目のログイン時は，認証情報生成種データは初期情報 D 0 であり，認証情報は D 1 である．

④ Y は，X から受信した認証情報を X の公開鍵で復号し，利用者毎に保存してある認証情報検査データと比較する．一回目のログイン時，認証情報検査データは初期情報 D 0 である．

⑤ ④の比較結果が等しければログインを許可し，X の認証情報検査データ格納場所に受信した認証情報を次回ログイン時の検査用として上書き保存する．不一致ならログインを拒否する．Y は，許可あるいは拒否いずれの場合でもその旨を X に通知する．

⑥ X は，Y から認証処理結果の通知を受けたら，ログインが許可されたか否かを確かめる．

⑦ 認証結果が許可であれば，認証情報生成種データ格納場所に，③で送った認証情報を次回のログイン時の認証情報生成種データとして上書き保存する．次回，X が再ログインするときは，保存した認証情報生成種データを X の秘密鍵で再度暗号化して新しい認証情報として Y に送る．二回目のログイン時は，認証情報生成種データは D 1 であり，認証情報は D 2 となる．

⑧ ①から⑦を繰り返す．

特徴は以下のとおりである．

・クライアントが秘密鍵を厳密に保管している限り，クライアントで保存している認証情報生成種データおよびサーバで保存している認証情報検査データを第三者が知っても認証情報を生成できないので「なりすまし」は不可能である．

・サーバのシステム管理者でさえ次回ログイン時に使用する認証情報を知ることができないので，利用者になりすますことはできない．

・第三者が送信中の認証情報を盗聴し再利用しても，サーバは既に認証情報検査データを更新済みなので「なりすまし」によるログインが可能な時間的隙間が無い．

・毎回異なる一回限りの認証情報を無限に生成可能である．

・認証情報として使用する公開鍵ペア更新時の初期情報登録作業が不要である．

・クライアントの公開鍵をサーバに配送するために認証情報と共に公開鍵証明書を送る方式を採用すれば，クライアントは任意に鍵を変更することが可能となる．

・認証処理シーケンスが単純である．

4） 生体特徴利用によるエンティティ認証

人の身体的特徴である指紋，声紋，手書き署名，タイピングパターンなどを認証情報として照合することにより本人であることを確認する（図 18）．

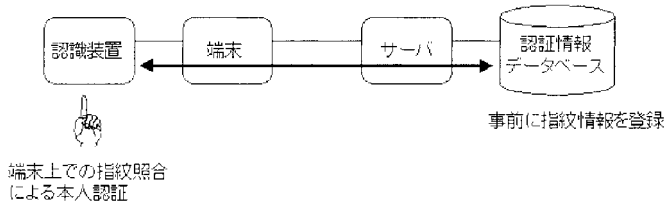


図 18　指紋認識によるエンティティ認証方式の例

長所には

・本人にしか持ち得ない認証情報として使用するので，認証が成功した場合の本人識別精度は高い．

がある．

短所には

・正当な本人であるのに認証が失敗することがあるなど認識確度が 100% ではなく，技術的な改良が望まれる．

・ネットワークを介した認証では盗聴により認証情報を再利用される可能性がある．

・個人の身体的情報が使われる心理的抵抗感があり，プライバシ保護が必要となる．

がある．

5）　所有物利用によるエンティティ認証

エンティティが所有する物（鍵，トークン，磁気カード，IC カードなど）に保持している認証情報によって検証する．

所有物は紛失や盗難などのリスクがあるので，ネットワークを介した認証ではサーバでの知識利用や暗号利用による認証と組み合わせて使用される．

長所には

・所有物を厳密に保持すれば「なりすまし」は困難である．

・IC カードは耐タンパー性があり，暗号鍵やパスワードなどの認証情報を比較的安全に格納・管理できる．またセキュリティ処理機能そのものを IC カード内に組み込むことでさらに安全な認証通信が可能となる．

がある．

短所には

・所有物と端末との間に専用機器が必要となることが多い．

・ネットワークを介した認証では知識利用や暗号利用を組み合わせているため，これらの短所も含んでいる．

がある．

図 19 に IC カードを使用した所有物利用の例を示す．この例では，液晶ディスプレイに現在時点のパスワードを表示する IC カードを利用している．IC カードと認証サーバとで同じ鍵を持ち，現在時刻を暗号化してパスワードを生成する．

6）　PKI（Public Key Infrastructure）による認証

PKI によるユーザ認証は，通信相手の電子署名と認証機関（CA）から発行された証明書をもっていることを確認することにより行う（図 20）．

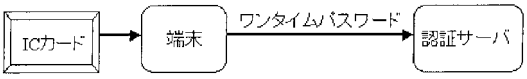


図 19　IC カードを使用した所有物利用の例

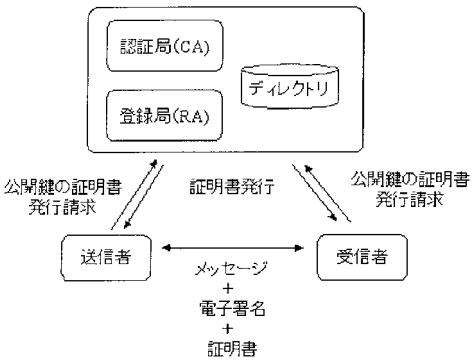


図 20　PKI による認証の概要

利用者は，公開鍵・秘密鍵のペアを生成し，その公開鍵と自分の身元を明らかにする情報を添えて申請する．認証機関は，申請された情報を元に身元の確認を行った後，電子的な「証明書」を発行する．証明書には，登録者の名前（識別子）や公開鍵，証明書の有効期限，証明書のシリアル番号，証明書を発行した認証機関の名称や認証機関の電子署名の情報が格納されている（表 4）．証明書は，認証機関の電子署名が付いているので第三者が偽造することはできない．認証機関が発行する証明書は ITU-T 勧告の X.509 v 3 が標準となっている．

認証機関の主な機能には以下がある．

・本人確認

認証機関は証明書の発行を申請してきた利用者の真正性を確認する．本人確認の際に必要とする情報は，企業の認証機関が従業員に証明書を発行する場合，クレジットカード会社の認証機関が会員に証明書を発行する場合，自治体が住民に証明書を発行する場合など，ケースによってさまざまである．

・証明書の発行と公開

本人確認後，申請情報に基づいて証明書を発行する．発行した証明書をリポジトリに登録して公開する．

・証明書の廃棄

秘密鍵が危惧化した，秘密鍵を紛失したなどなんらかの理由で有効期間内に証明書を無効にする必要が生じた際に証明書を廃棄する．廃棄された証明書は廃棄リスト（CRL：Certificate Revocation List）にのせてリポジトリで公開する．

・証明書の有効性確認

有効期間内であっても証明書が廃棄されている可能性があるため，証明書が有効であるかどうか利用者が確認できる手段を提供する．有効性確認の方法には，リポジトリに公開された CRL を調べる方法と OCSP（Online Certificate Status

表 4　証明書の記載項目

項目	内容
version	証明書のバージョン番号
serialNumber	同一 CA が発行した証明書をユニークに識別するためのシリアル番号
SignatureAlgorithm	証明書の署名アルゴリズム
issuer	証明書を発行した認証機関名(Distinguished Name 形式＊)
validity	証明書の有効期間
subject	公開鍵の所有者名(Distinguished Name 形式＊)
subjectPublicKeyInfo	所有者の公開鍵情報
issuerUniqueID	同一名の CA を区別するための識別子（Version2Only）
subjectUniqueID	同一名の公開鍵所有者を区別するための識別子（Version2Only）
extensions	拡張フィールド（Version3)。公開鍵ペアと証明書の使用目的に関する情報、証明書のポリシーに関する情報、ユーザおよび認証機関の属性に関する情報など

(＊)Distinguished Name 形式は、X.520 で規定されているディレクトリのネーミング方法。国名、地域、名前などの組み合わせでユニークな識別名を作る。

Protocol）によるオンライン有効性確認方法がある．

多種多様の認証機関がそれぞれの方針と運用規約に基づいてサービスを提供している．認証機関自身の信頼性を確保する方法として，自己保証，階層構造，相互認証がある．とくに，異なる認証機関から証明書の発行を受けている利用者間で相手を認証するためには，相手の認証機関の信頼性を確認できる相互運用性の確保が必要となる．

・自己保証　認証機関が自分自身を保証する．

・階層構造　階層構造の中で上位の認証機関が下位の認証機関を保証する．

・相互認証　複数の認証機関が相互に保証する．

自分自身を保証している認証機関をルート認証機関という．たとえば階層構造の最上位の認証機関はルート認証機関である（図 21）．

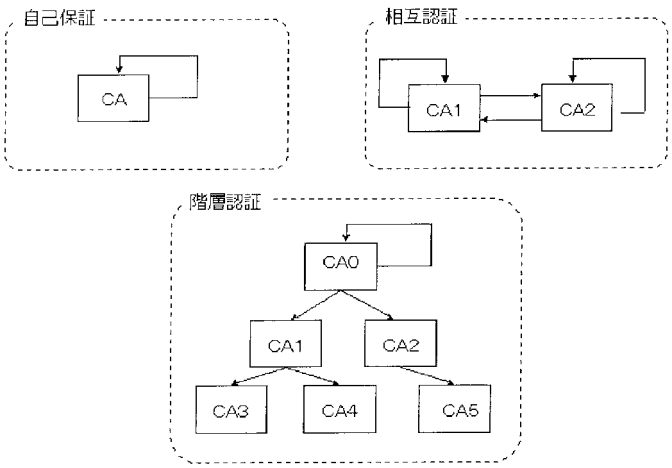


図 21　認証機関のモデル

電子署名の検証においては，証明書の有効性確認が相手の認証に重要なプロセスとなる．証明書自体が有効であるかは以下の項目を確認することが必要である．

・証明書の発行者が正しいこと
　認証機関の証明書自体が信頼できるか，あるいはその上位の認証機関や相互認証した認証機関を順に確認していき，信頼できる認証機関に到達できるかを確認する．
・証明書の内容が認証機関により保証されていること
　証明書自体が改ざんされていないことを認証機関の署名で確認し，かつ証明書の署名に用いられた認証機関の証明書も正しいことを確認する．
・証明書の使用方法が正しいこと
　証明書に記載された項目により，検証した時点が有効期間の範囲内であり，使用方法が制限事項や条件を満たしていることを確認する．
・証明書が廃棄されていないこと
　認証機関が提供する情報を利用するなどして，証明書の状態を確認すること．

とくに，証明書は正しく審査し発行されたとしても，秘密鍵の危惧化，証明書の記載内容変更などさまざまな理由によってたとえ有効期間内であっても廃棄されることがある．証明書が廃棄されていないかどうかを確認する技術には廃棄リスト（CRL）が広く利用されている．認証機関は発行した CRL をリポジトリに格納する．有効性を確認したい証明書を発行した認証機関のリポジトリから CRL を入手し，該当する証明書が載っているかどうか確認する．CRL による有効性確認は，データサイズが肥大化しがちなこと，実時間性に乏しいこと，さらに検証したい証明書に関係するすべての認証機関が発行した CRL を確認しなければならないといった欠点をもつ．これに対して認証機関がオンラインで有効性を確認する機能を提供するための OCSP が開発され，インターネット標準 RFC 2560 となって採用が広がりはじめている．OCSP では，証明書を OCSP レスポンダに提示して確認を要求し，OCSP レスポンダは該当する証明書の有効性を返送する（図 22）．

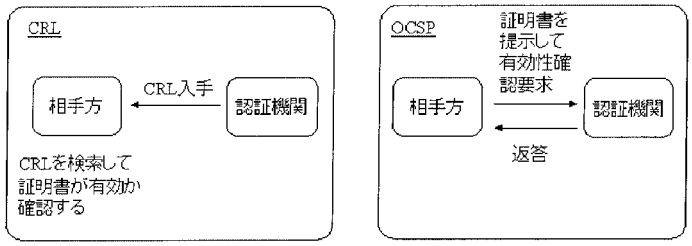


図 22　証明書の有効性確認手段

OCSP レスポンダは証明書を発行した認証機関以外のものでもよい．検証者は CRL を入手する必要が無い，証明書の廃棄情報がほぼリアルタイムに取得できるといった利点がある一方，OCSP レスポンダにトラフィックが集中する可能性があるなどの欠点もある[1]．

PKI による認証は，WEB サーバとクライアント間のセキュリティプロトコルとし

て標準的に使用されているソケットレベルのプロトコル SSL（Secure Socket Layer），電子メールでマルチメディアデータを扱うための標準フォーマット MIME をベースにした S/MIME（Secure/Multipurpose Internet Mail Extensions），標準化された VPN（Virtual Private Network）方式である IP レベルのセキュリティプロトコル IPSec など，広く利用されている．

＊1　FIPS：Federal Information Processing Standard
＊2　NIST：National Institute of Standards and Technology
＊3　付録は，文献［3］八津川直伸，UNISYS 技報 54 号，日本ユニシス株式会社，1997 年の一部を再掲，加筆した．
＊4　OSF：Open Software Foundation（オープンソフトウェア財団）

参考文献

［1］　電子認証システム推進検討会, 企業間電子商取引システムにおける電子認証システム仕様に関するガイドライン, 平成 12 年
［2］　宮川寧夫, 情報セキュリティ・マネジメントの実践規範・ガイドライン, IPA セキュリティセンター, 平成 12 年
［3］　八津川直伸, UNISYS 技報 54 号, 日本ユニシス株式会社, 1997.

執筆者紹介

多　田　宏　司（Hiroshi Tada）
1954 年生，1977 年東京教育大学理学部地学科地理学専攻卒業，同年日本ユニシス(株)入社．当社シリーズ 2200 用通信制御装置システムである，DCP/TELCON システムのオペレーティングシステム，ターミナルハンドラ，レジリエント機構および LAN 接続機構を中心に開発，保守業務などに従事する傍ら，大規模ネットワークシステム構築を担当．その後ネットワークサービスの適用業務担当を経て，現在，第一ソフトウェアサービスセンターネットワークサービス室長．

古　寺　　薫（Kaoru Furutera）
1957 年生，1980 年慶應義塾大学工学部管理工学科卒業，同年日本ユニシス(株)入社．グラフライブラリの開発，CASE ツールの企画，オブジェクト指向開発ツール TIPPLER の開発・保守，EC セキュリティの調査・企画等を経て，現在第一ソフトウェアサービスセンターネットワークサービス室に所属．