情報セキュリティ技術体系とその動向

Overview of and Trends in Information Security Technologies

才所　敏明　T. Saisho
遠藤　直樹　N. Endoh

企業・組織，および家庭におけるコンピュータネットワークの利用が一般化しつつある。さらに，このインフラ上で，多くの貴重な情報，機密文書・取引情報（電子決済情報，電子現金情報）などが扱われるようになってきた。このようなインフラを構成するハードウェア，ソフトウェア，データなどに対する犯罪は今後ますます増加するとみられている。情報セキュリティ技術は，この“情報”犯罪への対策としてきわめて重要である。単にあるシステムを守るだけでなく，われわれにとって身近かな社会生活が順調に営まれることを支援する技術ととらえられる。ここでは，情報セキュリティ技術の全体像を描き，個々の技術の役割を明示するとともに，技術の発展動向について述べる。

Computers and networks are now in widespread use in various organizations including enterprises and households. Because valuable information, such as confidential documents and information on transactions, is processed on this computer infrastructure, crimes related to hardware, software and data are expected to rapidly increase in the future.

Information security technologies are important as powerful countermeasures against such crimes. These technologies can be considered not only as protection for individual computer systems, but also as a means of facilitating the successful implementation of numerous social systems.

This paper provides an overview of information security technologies, explains why each technology is indispensable, and summarizes the trends in technological development in this field.

1 まえがき

情報セキュリティ技術の目的は，情報システム（コンピュータ，ソフトウェア，データ，ネットワーク）をさまざまな脅威から守り，機密性（秘密が守られている），完全性（壊れていない），可用性（いつでも使える）を保つことにある。

ここでは，この特集で扱う情報セキュリティの範囲を明示し，脅威の実例を取り上げてその対策としての情報セキュリティ技術の全体像を記述し，さらに個々の技術の発展動向を概観する。これにより，情報セキュリティ技術の社会における重要性を明らかにし，さらに後続の論文で紹介する当社の技術の位置づけを明らかにする。

2 情報セキュリティ技術の範囲

図1は，情報システムに対する脅威の原因（横軸）とその

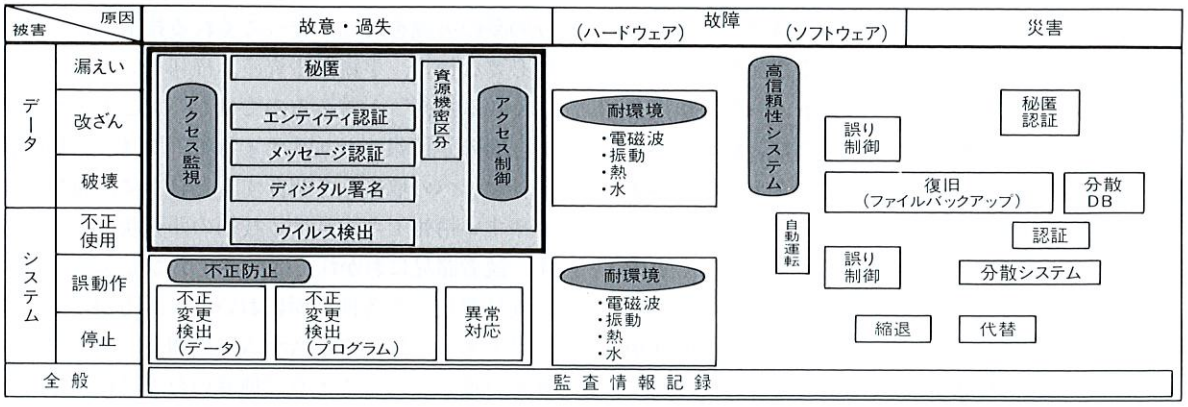

図1．情報セキュリティ技術の位置づけ　故意（悪意）・過失が原因で発生する，情報の漏えい・改ざん・破壊，およびシステムの不正な利用を阻止することが目的である。

Positioning of information security technologies

脅威によって発生する被害を示している。この特集では情報セキュリティの範囲として図1の網掛け部分を考えている。

3 情報システムに対する脅威の事例

最近の新聞報道に現れた脅威の事例として，パソコン通信事業者の管理するパスワードファイルが消去されたという事件がある。また，米国国防総省へのハッカ侵入は年間16万件以上と推定された。さらに，患者データを保管してある病院のパソコンが盗難に遭い東京秋葉原の電気街で売られていた，などもある。**図2**は，コンピュータの周囲で発生する脅威をまとめたもので，上述の事例も含んでいる。それぞれの事例に応じて，秘匿，認証，アクセス制御など，後述するさまざまな技術をどう利用するかを十分検討する必要がある。

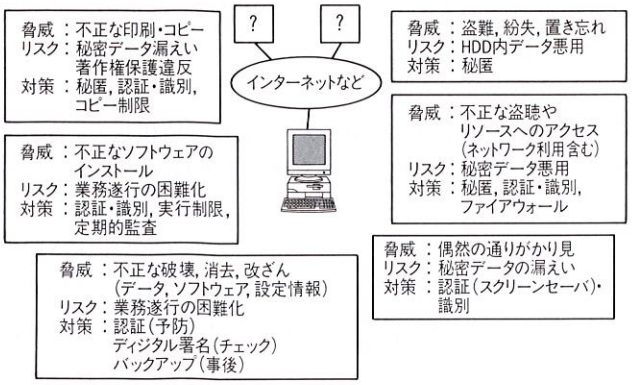

図2．コンピュータをめぐる脅威と主な対策　個々の情報システムの置かれた環境により，どの脅威が支配的かは一般に異なる。
Threats to computers and countermeasures

4 情報セキュリティ技術体系と発展動向

表1に情報セキュリティ技術の体系を示す。大きくは(1)秘匿技術から(7)セキュアシステム構築技術まで，7種に分類している。さらに7種の技術を主機能で分け，それぞれの機能に対応する手段として個々の詳細な技術体系を記述している。表1の秘匿，認証，識別の3種の技術は，情報セキュリティ技術の中の要素技術と位置づける。また，表1の(4)から(7)の技術は，要素技術のシステム応用という性格のものと監査や運用など人間の管理にまで波及する性格のものからなっている。

以下，7種の技術とその動向を説明する。

4.1 秘匿技術

いわゆる暗号技術であり，秘密鍵(かぎ)暗号と公開鍵暗号がその根幹である。両者は，暗号化と復号の鍵が同じか異なるかで分けられる（**図3**）。

表2に示すように，相反する長所と短所をもっているため，目的に応じて組み合わせて使うのが一般的である。高速処理が可能であるが秘密鍵の配送を必要とする秘密鍵暗

表1．情報セキュリティの要素技術とシステム技術
Fundamental and system technologies for information security

	技術分類	主機能	技術体系	
要素技術	(1) 秘匿技術	内容秘匿	秘密鍵暗号による秘密通信 ブロック暗号／ストリーム暗号	
			公開鍵暗号による秘密通信やディジタル署名	
			ハッシュ関数による署名作成用圧縮	
			鍵管理技術　鍵配送／鍵保管	
		暗号システム	電子商取引システム，鍵預託システムなど	
	(2) 認証技術	エンティティ認証	暗号を用いた相手認証プロトコル （個人・端末など通信相手の正しさの確認）	
		メッセージ認証	秘密鍵暗号＋ハッシュ関数など （メッセージの改ざん・でっち上げの検出）	
		ディジタル署名	公開鍵暗号 （メッセージの作成者の特定）	
	(3) 識別技術	個人識別	記憶利用型　パスワード	
			所持品利用型　カード	
			肉体的特徴利用型	指照合 顔画像照合 指紋・虹彩照合 など
		機器識別	機器識別情報の安全な埋込み	
システム技術	(4) アクセス制御技術 アクセス管理技術	情報やインフラの不正利用防止	情報システムアクセス制御 ・認証システム技術 ・認証ドメイン連携技術	
			ネットワークシステムアクセス制御 ・ファイアウォール	
			コンピュータアクセス制御 ・セキュア telnet，login	
			CPU アクセス（実行）制御 ・不正プログラム検出／実行防止	
			DB アクセス制御 ・アクセスコントロールリスト	
			ファイルアクセス制御 ・セキュア共有ファイル ・セキュアファイルシステム	
			アプリケーションアクセス制御	
	(5) 情報管理技術 情報フロー制御技術 耐タンパ技術	情報通信インフラ上の情報秘匿	情報管理／フロー制御 ・セキュア PC ・著作物管理（公証/コピー防止/改ざん防止など） ・暗号メール／セキュア ftp ・セキュア wais/gopher/www	
			情報フロー監視／追跡 ・鍵管理／否認防止技術	
			耐タンパ技術 ・攻撃検知／攻撃技術	
	(6) 監査・追跡技術	不正利用の検知および犯人追跡	監査機能 ・組込み／実行技術 追跡機能 ・組込み／実行技術	
	(7) セキュアシステム構築技術	セキュリティの SI 手法提供	セキュアシステム構築のための ・リスク分析／評価 ・方式検討／設計 ・運用方式／基準設計 ・セキュア開発環境構築 ・開発成果物の安全性保証 ・セキュアレベル評価／システム整備	

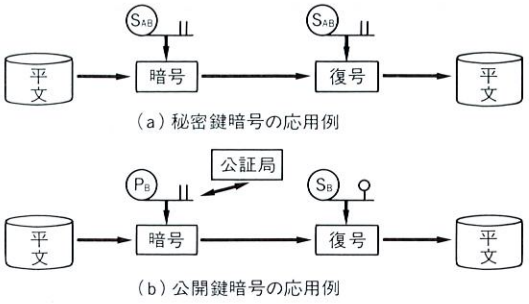

図3．秘密鍵暗号と公開鍵暗号の基本的利用法　秘密鍵暗号は暗号と復号の鍵が共通，公開鍵暗号では共通でない。公開鍵には通常公証局のお墨付きが必要。

Use of symmetric and public-key cryptography

表2．秘密鍵暗号と公開鍵暗号の比較

Comparison of symmetric and public-key cryptography

	秘密鍵方式		公開鍵方式
原理	暗号化鍵＝復号化鍵 （秘密）　（秘密）		暗号化鍵≠復号化鍵 （公開）　（秘密）
秘密鍵の配送	必要（×）		不要（○）
所有する秘密鍵の数	多い（×） 通信の相手の数だけ必要		少ない（○） 通信相手の数に関係なく自分の一つの鍵だけ
安全な認証	困難（×）		暗号と表裏の関係（○）
暗号化速度	高速（○）		低速（×）
アルゴリズム	秘密	公開	公開
代表例	Clipper	DES	RSA
主な用途	秘密通信 外交	多分野での情報秘匿	認証， E-mail の電子署名

号はデータ自体の暗号化に，処理速度は低いが秘密鍵配送が不要な公開鍵暗号は相手の確認に用いられる。

もっとも有名な秘密鍵暗号は1977年に発効した米国のDES（Data Encryption Standard）であり，多くの応用事例がある。しかし，56ビットという鍵の長さは，コンピュータの計算能力の目覚しい発展に伴い不十分になってきたと言われており，triple-DESという鍵長112ビットの暗号や鍵長128ビットクラスの暗号が今後主流となってくる。公開鍵暗号では米国産のRSA方式がある。電子決済や電子現金など相手確認の要求が厳しい分野でますます多用されることになろう。

4.2　認証技術

暗号アルゴリズムによって，通信相手の正しさの確認（共通の秘密をもつことの確認），メッセージの完全性検証，情報発信者の特定（署名）などを実現する技術である。データを秘匿して通信する場合のメッセージ認証や，ディジタル署名の用いかたを図4に示す。この分野では，トランザクションの発生量が増えることに対応できる高速な署名方式の開発や，ユーザの情報を開示することなく認証を行う零知識証明の応用などが進むとみられる。

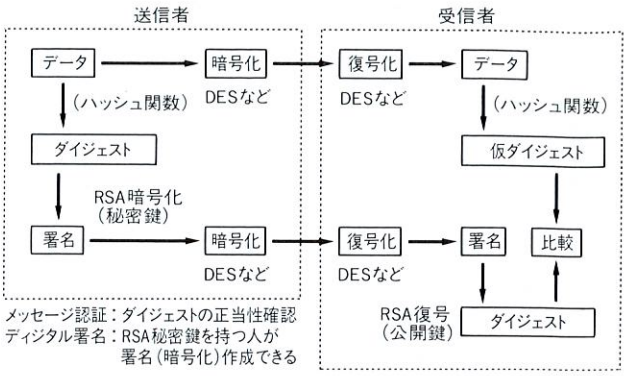

図4．暗号通信システムの構成例　データの暗号化に加えて，ダイジェストによるメッセージ認証や公開鍵暗号によるディジタル署名が利用される。

Example of data encryption system configuration

4.3　識別技術

情報システムの利用者を特定する技術である（図5）。従来は，正しいパスワードを知っていること，正しい磁気カードをもっていること，などにより特定していたが，パスワードの盗聴や磁気カードの改ざんなどの事例が増えており，よりセキュアな方式が求められている。一つは，電子商取引の世界で不可欠なICカード技術や情報システムの設置してある場所への出入りを制御する非接触カードの技術である。もう一つは，カードの正当な持ち主であることや部屋に入ってよい人かどうかを直接確認できる生体特徴による個人識別技術（指形状，顔，指紋など）である。この特集では，これらの技術に対する当社の取組みを詳述している。

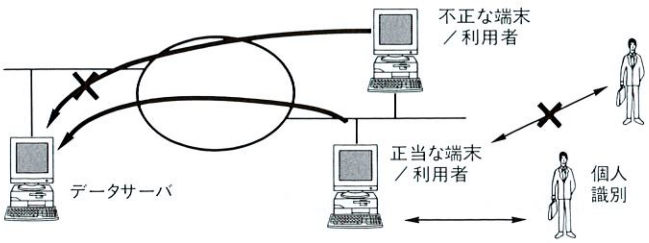

図5．利用者認証・個人識別技術の機能　不正な端末や利用者が貴重なデータにアクセスするのを防ぐ。

Function of entity authentication and personal identification technologies

4.4　アクセス制御技術

情報システムを構成するさまざまな要素（システム全体，ネットワーク，コンピュータ機器，データベース，CPU，ファイル，ソフトウェアなど）に対するアクセスを管理する技術である。秘匿，認証，識別などの技術をその要素技術としたシステム技術ととらえる。図6は，インターネット

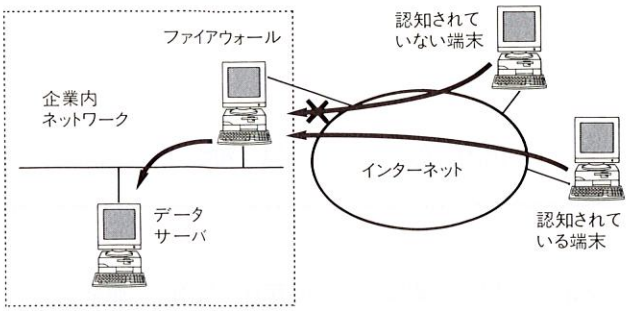

図6．ファイアウォールの機能　認知されている端末に対して，特定の許可されたサービスだけを提供するのが基本機能である。
Function of firewall system

など不特定多数が利用するネットを経由した企業内ネットワークへのアクセスを管理するファイアウォールの機能を示している。

4.5 情報管理技術

情報システム上でもっとも大切でしかもアタックを受けやすいと思われる情報（データ，ファイル，および鍵など）そのものの保護のためのシステム技術である。暗号・認証技術がその要素技術となる。

この特集では，クライアント／サーバシステムでのファイルの共同編集やバージョン管理を安全に行えるセキュア共有ファイルを詳細に述べている。また，携帯パソコンや共同利用パソコンのファイル秘匿をきわめて少ない操作で実現できるPCファイル暗号化システムも紹介している。さらに，分散環境ミドルウェアの上に構築したセキュアなWebシステムの技術も紹介している。これら当社の特長技術は，上記のアクセス制御や情報管理の技術に該当している。

4.6 監査・追跡技術

情報システムが不正なアクセスを受けたときに管理者がそれを認知できたり，または，どこからのアクセスかを調査できるようにする技術である。

4.7 セキュアシステム構築技術

対象となる情報システムの特性を把握しシステムに導入すべきセキュリティ手段を設計，実現し，さらにその適切な運用により，機能の活用を図る総合的な技術である。

監査・追跡技術およびセキュアシステム構築技術は，ソフトウェアやハードウェア以外の人間管理の面が強い。企業においては，ビジネスに成功するために，情報システムとそれにかかわる人間は常時どうあるべきか，という面からの考察が必須(す)であり，ビジネスプランニングやリスクマネージメントの一形態としてもとらえるべきである。ネットワークのオープン化やダウンサイジングの結果，ベテランのネットワーク管理者であっても自己の責任範囲が変化してきているという認識をもって管理を行う必要が出てきている。

5 情報セキュリティ技術の標準化動向

最後に，情報セキュリティ技術に関する世界レベルでの標準化動向について整理する。標準化は主にISO（国際標準化機構）の研究グループ（SC）で行われている。主なものは，① SC6（通信と情報交換），② SC17（ICカードほか），③ SC21（開放型システムでの情報転送・検索・管理），④ SC27（セキュリティ要件・サービス・技術・機構）などである。ただし，暗号アルゴリズムについては，標準化対象ではなく登録制となっている。

また，コンピュータシステムのセキュリティ評価基準と言われるものが，米国，欧州，豪州，日本など世界各国で作成されており，例えば米国では政府調達物件のセキュリティレベル評価の指針として利用されている。わが国では，日本電子工業振興協会（JEIDA）が1994年にまとめている。現在はこの基準を用いてセキュリティレベルを評価するための具体的な仕組みが検討されている。世界的には，各国の基準をCommon Criteriaという共通の基準にまとめ上げる作業が進められている。

当社は，ここで述べたISOでの標準化作業やわが国におけるJEIDAでの検討作業全般に対して，要員を派遣するなど積極的に参画している。

6 あとがき

ここでは，この特集における情報セキュリティの範囲を明確にした。また，世の中で実際に起こっている情報セキュリティの脅威を紹介するとともに，予想される脅威の全体像をまとめた。次に，その対策としての情報セキュリティ技術を概観し，最近の技術開発動向をまとめた。最後に，ISOなどにおける標準化のようすを簡単に紹介した。

当社は，すべての情報システムユーザが正当な成果を得ることができる環境をより完全なものにするため，有用な情報セキュリティ技術の開発，商品化に邁(まい)進する所存である。

才所　敏明　Toshiaki Saisho

研究開発センター 情報・通信システム研究所部長。
暗号・情報セキュリティの研究開発に従事。情報処理学会，CSI，ACM，IEEE各会員。
Communication & Information Systems Research Labs.

遠藤　直樹　Naoki Endoh

研究開発センター 情報・通信システム研究所主任研究員。
暗号・情報セキュリティの研究開発に従事。電子情報通信学会，セキュリティマネジメント学会会員。
Communication & Information Systems Research Labs.