情報社会におけるセキュリティの重要性とその確保について

住友化学システムサービス㈱
雪　浦　和　雄

The Importance of Security and Security Policy in Information Society

Sumitomo Chemical Systems Service Co., LTD.
Kazuo Yukiura

I explain the importance of security in information society and what types of security threats. I present recent examples of actual security breaches both inside and outside the company. The first security measure that should be undertaken is to establish a security policy for the enterprise. Each item of security policy is explained, providing high-level and low-level examples. Finally I explain ISO 15408, an international security certification criterion.

はじめに

情報社会におけるセキュリティの持つ重要性とセキュリティに対する脅威を解説する。過去の社内外の事例を挙げ、セキュリティに対する侵害が身近に起こっていることを紹介する。セキュリティ対策として、最初に行うべきことは企業のセキュリティポリシーの策定である。その定めるべき内容について高いレベルと低いレベルを例示しながら項目別に解説する。最後にセキュリティの国際標準である、セキュリティ評価認証制度 ISO15408 について紹介する。

セキュリティとは

1．セキュリティの重要性

情報は企業にとってもっとも貴重な資産であり、研究報告、設計図面、営業情報等各種の重要な情報を社外および社内への漏洩から保護し、維持する必要がある。また顧客情報は企業の貴重な資産である一方、顧客のプライバシーでもある。顧客のプライバシー情報の漏洩は企業のイメージダウンを招き、信頼を失墜させてしまう。電子商取引（EC）への参加権を得るためには、自社がセキュア（安全）なネットワークを持つことが不可欠の要件となっている。企業がインターネットを通して直接個人消費者に販売を行う形態 B to C の場合には、悪意のある利用者は、他人への成りすましや取引事実の否定等の手段によって企業に損害を与えることができる。またサイバーテロによって企業情報システムが麻痺する、あるいは企業情報が破壊される危険もある。

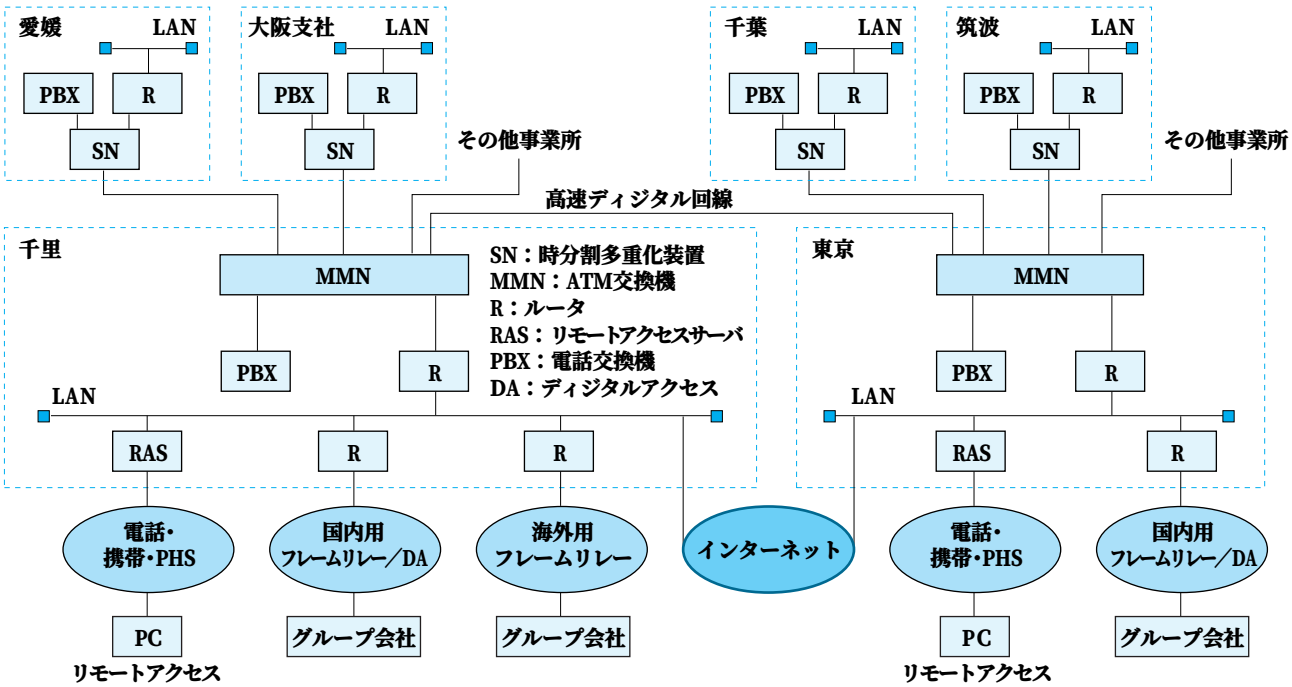
セキュリティ対策とは単に情報の漏洩や破壊の防止のみでなく、障害による情報喪失を含め、企業活動のリスク管理そのものである。

2．ネットワークの現状と今後の発展

ネットワークセキュリティが問題になる背景として、企業内ネットワークの拡大、グループ会社間によるネットワークの共有化の進展、他企業との接続発生といったことがあげられる。住友化学においては1992年に大阪本社にインターネットメールサーバを置き、研究所で使用されていた一部の UNIX とパソコンを利用してインターネットメール、ニュースの利用を開始した。その後クライアント・サーバ方式と呼ばれる分散処理型のコンピュータシステムの登場とともにネットワークが拡大していった。特定の部門の人が利用していた電子メールは PC の全社的な導入により急速に普及し、全社員が利用できるようになっており、その利用回数は毎年確実に増加している。

現在の住友化学グループのネットワーク（SCNET）を第1図に示すが、国内の住友化学の全事業所13箇所、グループ会社44社、海外は北米、ヨーロッパ、アジア（シンガポール）等7箇所が専用線あるいはフレームリレー回線で接続されている。国内ではネットワークへの接続（アクセス）は携帯端末（モバイル）利用により、電話、携帯電話、PHS、ISDN（64Kbps）を用いて全ての地域から可能になっている。海外には電話、携帯電話を利用したリモートアクセス可能な設備が3箇所用意されている。

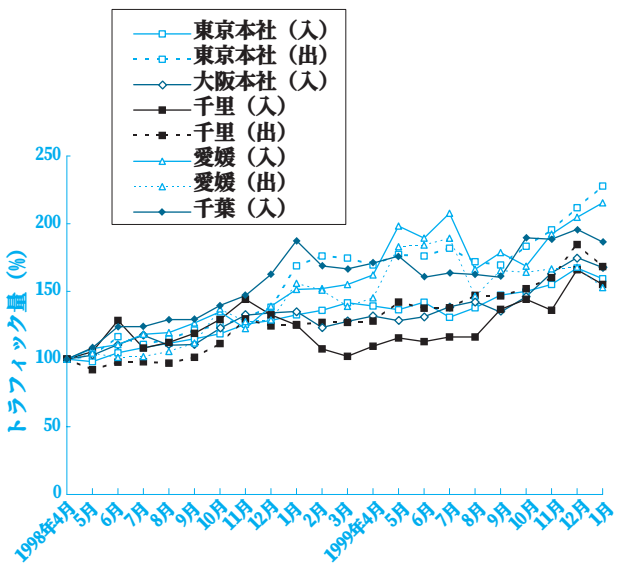
第１図　住友化学グループのネットワークの(SCNET)概要図



3．利用形態の多様化と通信量の急激な伸び

事業所間の通信のデータ量をみて見ると、第２図にあるように着実に増加している。事業所間の通信量は増加が激しい個所では３年間で３倍になっている。またインターネット用の回線速度は1992年スタート時はモデム回線を使用し回線速度約30kbpsであったが、現在は1500kbpsに拡大されている。インターネットの利用者数はこの数年急速に増加している。世界のインターネットの利用者は過去３年間で３倍以上に増え1億人を超えそうな勢いである。このようにネットワーク、インターネットの重要性は益々高まっている。

第２図　1998年度－1999年度ネットワークトラフィックの遷移



セキュリティと脅威

1．脅威の分類[1)]

ネットワーク化した社会における情報のセキュリティに対する脅威を現象面で大きく分類すると次のようになる。

（１）暴露

不正にデータの内容が露見すること。許可をされていない利用者がデータ・ファイルにアクセスしたり、データの保管媒体を持ち出すことにより発生する。

（２）破壊

不正にデータを削除されたり、使用不可能な状態にされること。許可されていない利用者がデータファイルを削除したり、データ転送中の中継システム上でデータを削除することによりデータ破壊は発生する。コンピュータウイルスの侵入等によりデータを格納している媒体（ハードディスク等）が破壊されたり、システムのハードウェアに障害が起きてデータが破壊されたりもする。

（３）過負荷（オーバトラフィック）

不正にデータの処理を妨害され、許容レスポンス範囲内で処理ができなくなること。処理対象としては無関係な不要データを大量に入力されると発生する。インターネット利用におけるメール爆弾という手法では、不要なメールが大量に送りつけられて、それを受け取ったメールサーバの正常な処理が妨げられる。

（４）拒否

データを処理した事実や、処理したデータの結果を後から拒否されること。データ処理の事実を記録するログデータの収集を妨害されたり、ログデータの内容を改ざん・破壊されたりすると発生する。たとえばインターネットの通信販売の契約書や発注書、企業間のEDI（電子データ交換）の受発注などを扱う場合に、ログデータが消されると、発注の事実を否定されてしまう。

（５）ユーザ認証に関する脅威：成り済まし

許可されていないユーザが許可されたユーザに成り済ます。たとえば、本人に成り済まし、他人が不当に業務アプリケーションを実行する。通常は成り済ましを防止するために、ユーザを識別して認証する仕組みを設けて対処する。しかしこの仕組みを設けても次のような脅威がある。

- 識別／認証情報を盗む。例としてはパスワードを盗む、あるいは盗み見る。
- 識別／認証情報を類推する。生年月日等からパスワードを類推する、あるいは辞書を用いて、ありそうなパスワードを類推する。
- 暗号化された識別・認識情報を盗み、そのデータをシステムに再送して、許可者に成り済ます。

2．具体的な過去の事例

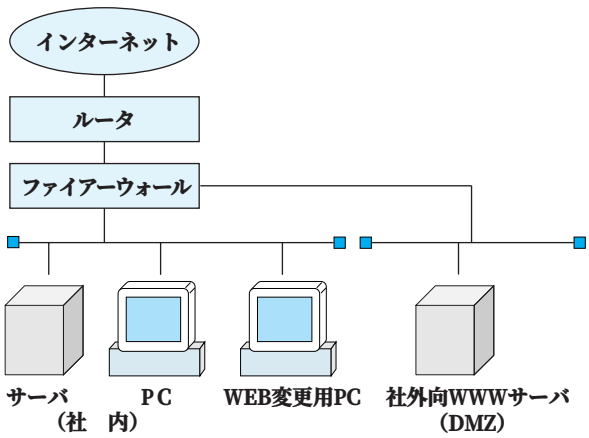
以下に脅威の実例を住友化学グループ内の設備の現状、課題を一部交えながら紹介する。

（１）インターネットからの侵入によるホームページの改ざん

今年１月末の日本のニュースで大きく取り上げられた科学技術庁他のWWWサーバのホームページ改ざん事件は多くの人の注目を集めた。その理由は中央官庁のシステムのセキュリティ対策は万全と多くの国民が思っていたにもかかわらず、WWWサーバが同時に複数改ざんの被害に遭ったということであろう。不正アクセスの手段は前述した手法でパスワードを取得し、改ざんしたと推定されている。通常はWWWサーバは第３図のようにファイアーウォールと呼ばれる装置で外部および社内内部から隔離されて置かれ、それぞれからの不正アクセスを防御している。外部からWWWサーバのホームページを変更出来ないように、社内内部からの変更は特定のPCからかつ特定の管理者以外はできないようにアクセス制限をかけている。

官庁のホームページがハッカーにより改ざんされた原因はファイアーウォールがなかったケースと、ファイアーウォールは設置していたが、ホームページを社外から更新するためのファイアーウォール上のパスワードが解読されたケースの２つがあると言われている。

第３図　ファイアーウォール



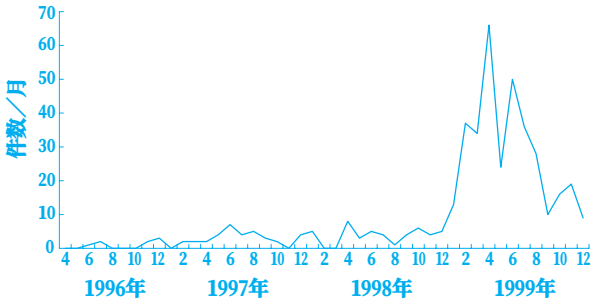
（２）コンピュータウイルスによる被害

EXCEL.Laroux と呼ばれるマクロウイルスが1997年２月に住友化学のSCNET上のパソコンに侵入し第１表のような被害を与えた。この時点はウイルス対策ソフトが全PCに導入されていたが、ウイルスの検出が実質できず、発見、駆除ともに多くの時間と労力を要した。過去４年間の住友化学におけるのウイルスの検出状況を第４図にまとめた。ウイルス対策ソフトをインターネットの入り口と全PCに導入した結果、第４図からわかるようにウイルスの検出件数は確実に増えているが、その後の被害は１件のみである。これはウイルス対策ソフトを導入した効果であり、かつウイルス対策ソフトの品質が上がってきたためと推定される。

第１表　EXCEL.Larouxによる被害状況

発見	1997年2月25日
ウイルス名	EXCEL.Laroux
被害状況	感染PC 64台
発生事業所	東京、大阪両本社を含む10事業所
発見と駆除	ウイルスバスター95で発見、手作業による駆除

第４図　住友化学ウイルス検出件数



（３）インターネットの過負荷

あるPCがインターネット経由で動画像であるMPEGファイルをダウンロードしたために、住友化学向けのインターネット回線が2時間半にわたってほぼ100％利用の状態になった。メールや他のWWW参照と競合しながら、ダウンロードが進んだので致命的な影響は無かった。現状の対策は運用規制（利用者の自粛）であるが、将来的にはダウンロード容量の自動的な制限が必要と思われる。インターネットメールの容量制限はすでに実施している。

住友化学のセキュリティ対策状況

1．外部コンサルティングによる診断

1999年に㈱NTTデータに住友化学のセキュリティ診断を依頼した。多くの指摘事項を受け、可能なものは対策を実施した。本来定めておくべき事柄が抜けていたり、社内では当たり前と思っていることが、問題であると指摘されるなど、非常に有益な指摘が多く、対応すべきことが多かった。一例を挙げると緊急事態発生時の対策プラン（contingency plan）が作られていないとか、容易にパスワードクラックされるパスワードの存在の指摘があった。

セキュリティポリシーの制定と住友化学及びグループ会社の現状

1．セキュリティポリシーの制定の必要性[2,3,4]

企業においては、セキュリティポリシーを制定し、機密情報を含む企業の資産をどのように管理、保護、流通させるかを規定した規則、その実施方法を定める必要がある。何をどのような脅威から守り、そのために何をすべきかについて明文化する必要がある。

このように定めたセキュリティポリシーに基づき、具体的なセキュリティ対策、詳細な運用規則を決定していくことになる。企業のタイプによりセキュリティポリシーは大幅に変わる。金が沢山かかっても企業の情報を守らなければならない組織（例：金融業）と金はあまりかけたくないが、外国を含め外界から情報取得を容易に行いたい、外界とのコミュニケーションを積極的に行いたい組織（大学、研究機関）とではそのポリシーは大きく異なる。インターネットとつなぐかどうか、他企業とつなぐかどうか、自社のグループ企業とつなぐかどうかもその企業の性格により変わってくる。セキュリティポリシーは企業のトップの意志を反映した形で組織内の合意を得て決定され、確実に守られる必要がある。

以下セキュリティポリシーの主要な項目について各項目の意味とサンプルを紹介する。その中で、高いセキュリティレベルを維持するためのポリシーと低いセキュリティレベルを維持するためポリシーの例を説明する。

2．認証[5]

アクセス制限をかけたいシステムに対しては、アクセスする場合に、ユーザIDとパスワードによって利用権を確認する（認証を行う）。厳しい基準で運用する例を挙げると次のようになる。パスワードは6文字以上とし、辞書に載っている単語は使用しない。英語、数字、記号を混ぜる。パスワードを5回続けて入力ミスをしたらそのユーザIDは使用停止にする。15分間以上やり取りのないセッション（会話モードでの接続）を無効にし、再度認証を要求する。前回のログオン日時を表示し、他人が使用していないことを確認できるようにする。一定期間使用していないユーザIDは廃止する。パスワードは設定変更後一定期間が過ぎた場合、必ず変更を求め、変更しないとログオンできなくする。実際には上記内容を全て実施するとパスワード忘れる人が続出、あるいは人目につくパスワードのメモが発生する等の問題があり、まず利用者のセキュリティ意識を向上させる必要がある。システムの重要度を考慮し、実施内容を決定する。住友化学内スターオフィスの利用の場合では、一部しか実施されていない。

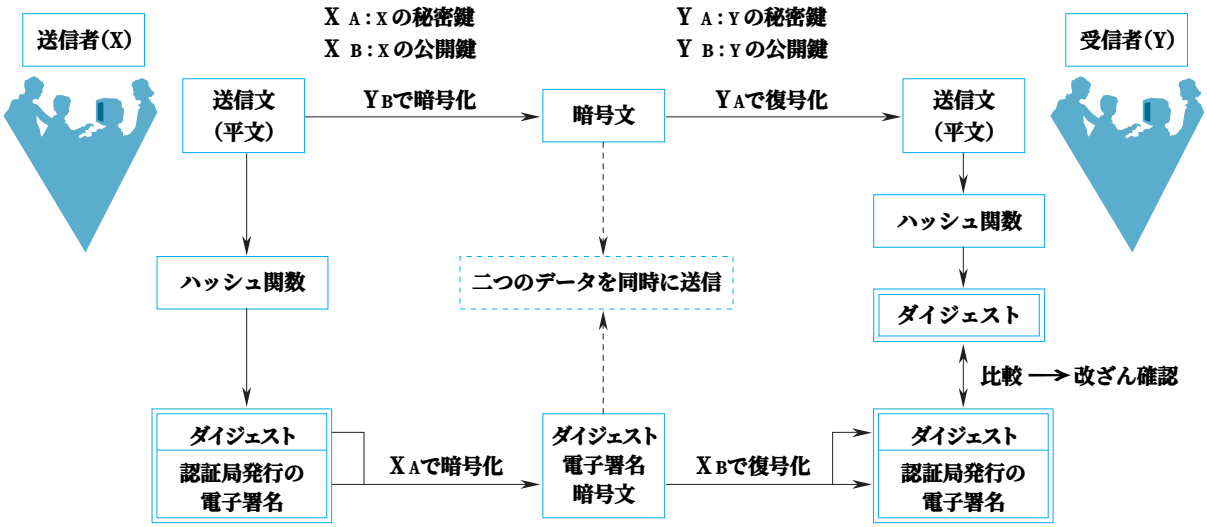
電子商取引などでより高いセキュリティの認証が必要な場合には、電子署名を採用する。

第5図に電子署名の仕組みを紹介する。電子署名を利用する場合には証明書の発行が必要になる。現在すでに商用化されており、信用のある商用機関から証明書が発行されている。電子署名の証明書は通常パソコンに埋め込まれて使用するので、パソコンが盗まれて使用されるのを防ぐために、前段で説明したパスワードを使用している。最近はディジタル証明書を収容したスマートカードと呼ばれるICカードまたはハードウェアトークンが使用され始めており、今後の普及が予想されている。

（１）電子署名の紹介[6]

メッセージの出所と送信者の身元の両方を確認するためにディジタル署名として知られる認証（オーセンティケーション）ツールを使う方法がある。第5図に示すように、ディジタル署名はハッシング（データを短いものに変換すること）アルゴリズムを用いて送信文からダイジェスト文（短いメッセージ）を作り、それを後で説明する公開鍵暗号化システムを用いて送る。具体的にはダイジェスト文を送り手の秘密鍵で暗号化する。これと送信文（平文）を一緒に送る。受信者は送信者の公開鍵で暗号化されたダイジェスト文を復号

第５図　電子署名と証明書の発行



化して、それを受信したメッセージから同じハッシングアルゴリズムを用いて再作成したダイジェスト文と比較する。一致していれば、送り手が本人であることおよび送られた文書に改ざんが無いことがわかる。

送り手の公開鍵をどのようにして入手するかは2つの方法があり、1つは信用ある商業ベースの認証サーバ（ベリサイン社、サーバートラスト社等）を利用する方法であり、もうひとつは企業が自身で認証サーバを立ち上げる方法である。

3．ソフトウェアの導入

ソフトウェア導入に伴い発生する脅威としてはウイルス、JavaやActiveXの会話形プログラムの実行、ソフトウェアライセンス無しでのプログラム不正使用等があり、それぞれに対してセキュリティ制御をかける必要がある。

（１）ウイルス対策（予防、検出、駆除）

高いレベルのセキュリティでは、下記の対策を実施する。インターネットからのウイルスを防ぐためにウイルスチェックプログラムをインターネットの入り口に置きウイルスの侵入を防ぎ、すべてのサーバ、パソコンにウイルスを検出するソフトを載せる。個人の判断によるソフトウェアの導入を一切認めず、セキュリティ管理者のみが導入を認証したソフトウェアのみ、該当パソコンへの導入を許すようにしている。ウイルスの検出ソフトを毎日実行することを義務付けている。住友化学においてはほぼ高いレベルの実施がなされているが、サーバの多くはまだウイルスチェックソフトはインストールされていない。現在導入中のExchangeサーバにはインストールされている。インターネット入り口のウイルスソフトの検索エンジン、パターンファイルはインターネットから自動的にインストールされており、パソコンの検索エンジン、パターンファイルも各事業所のインストール用サーバを更新することによりユーザが意識することなく自動的に更新されている。

（２）会話型プログラムのセキュリティ対策

Javaと呼ばれるサンマイクロソフトが開発した言語を使用してプログラムを作成すると、インターネットからそのプログラムをダウンロードし、それをパソコン上で実行することができる。Javaはセキュリティを十分考慮して作った言語なので、通常はそのPCのディスク等を破壊することはない。しかしセキュリティホールと呼ばれるJavaのバグがあり、悪意のある人がそれを利用してプログラムを作ることによりPCのディスクを破壊することもできる。セキュリティホールは逐次対策され埋められているので危険は小さくなりつつある。マイクロソフトが開発したActiveXはJavaと同様な機能を持っているが、PCとダウンロードするサーバ間で信頼関係を結ぶとディスクへのアクセスを含めPC上であらゆる操作が可能である。高いセキュリティを要求する企業ではファイアーウォールですべてのJava、ActiveXをブロックするかもしれない。次にセキュリティが高いレベルではファイアーウォールは信頼できるサーバからのみダウンロードを許す。

（３）ソフトウェアのライセンス管理

セキュリティの高いレベルでは、システム管理者の承認の無い商用ソフトのインターネット経由でのインストールは一切認めない。会社内のコンピュータ上で使用する全てのソフトウェアはライセンス管理、契約管理を行い、システム管理者がインストールする。セ

キュリティの低いレベルでは、ユーザが承認手続きを取り、ライセンスを取得し、ユーザ自身でインストールする。住友化学の現状は規定としてはシステム管理者が承認を与えたプログラムを、システム側で購入しインストールを許可している。従ってセキュリティレベルは中間のレベルになる。

4．暗号化

インターネット上で交換しようとする情報のセキュリティを考慮すると、送信時に暗号化し、到着時に復号化する方法がもっとも効果的である。しかし暗号化に関しては、暗号化を許可しない国もあり、運用面ではデリケートな難しい問題を含んでいる。たとえば米国は自国内ではセキュリティが高い（暗号が解読される危険性が極めて低い）トリプルDESと呼ばれるキー長が112ビットの暗号化の使用を認めているが、海外への輸出はキー長がずっと短い40ビットしか認めていない。しかし40ビット長では時間をかければ比較的容易に復号化されることが実証されており、絶対に安全とは言えない。一方解読に要するコストを考えると、40ビットでも実用上ある程度は安全であるという判断もできる。フランス、中国は暗号化そのものを認めていない。今後の方向は、社会のニーズが強いこと、よりセキュリティの高い米国製以外の暗号化製品が登場しており、それらは輸出されている等の背景があり、特定の国への輸出を除き、輸出解禁が間近いと思われる。国別の法的規制にバラツキがあるので実際の運用では慎重な調査が必要である。

重要なデータ（特にconfidential data）は最低キー長56ビットから75ビット以上で暗号化すべきであるといわれている。また暗号化で使用するキーの厳正な管理が重要である。

（1）リモートアクセス

電話（正確には通常の電話、携帯電話、PHS、ISDN）を利用したダイアルインによるリモートアクセスとインターネットを利用したリモートアクセスがある。

高いセキュリティを要求する場合では、企業秘密の情報を送る場合は電話経由であろうがインターネットであろうが暗号化が必要である。住友化学の場合は現状はRAS／DSS、国内専用にはNNCSを使用しているが、共に本文は暗号化されていない。

（2）Virtual Private Networks　VPN

VPNは情報漏洩に関して信頼性の低いインターネットを用いて、信頼性の高いネットワークと信頼性の高いネットワークとの接続を可能にする方式である。ファイアーウォールの技術がVPNを実現している。VPNで使用される全てのネットワーク接続はネットワーク管理者の承認が必要であり、暗号化キーのメンテナンス方法も運用に入る前に決めておく必要がある。住化においてはVPNのテストは完了しており、現在導入に向けて準備中である。世界のどこであろうが、インターネットのある地域ならVPNは利用可能であり、住化のネットワークへアクセス可能である。ミッションクリティカルな（必ず即時に到着・処理する必要がある）業務の用途にはVPNを用いてはいけない。高いセキュリティを要求する場合には、VPNが止まった場合の代替のネットワークを用意しておく必要がある。

（3）共通鍵暗号化方式と公開鍵暗号化方式の紹介

今後利用される暗号化方式を紹介する。暗号化方式のひとつに共通鍵暗号方式がある。平文（P）を共通鍵（K）を用いてアルゴリズム（E1）により暗号化する。暗号化された文を（A）とすると

$$A = E1(K, P)$$

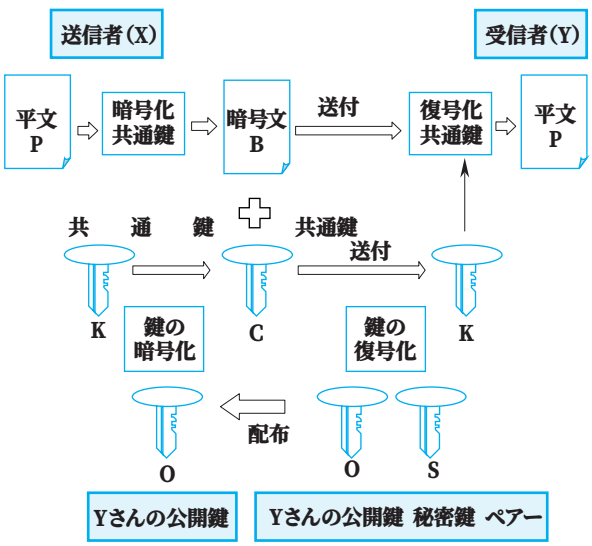
となる。暗号を復号するために同じ共通鍵（K）を用いて暗号化された文（A）をアルゴリズム（E2）を用いて復号化する。

$$P = E2(K, A)$$

この方式は対称的鍵システムとも呼ばれる。

これに対して公開鍵暗号化方式は公開鍵と秘密鍵とを使用するシステムである。公開鍵、秘密鍵はそれぞれ全ユーザに1つずつ与えられる。公開鍵は公然と知られ公表されている。秘密鍵は各ユーザが秘密にしておかなければならない。もっとも良く知られている共通鍵と公開鍵を用いた暗号化方式にRSAアルゴリズムがある。第6図参照。送り手はまず先に紹介した共通

第6図　共通鍵と公開鍵の組み合わせによる暗号化



鍵アルゴリズムを使って自分の平文を共通鍵（K）を用いて暗号化する（メッセージB）。次に受け取り者の公開鍵（O）を使って共通鍵（K）を暗号化する（メッセージC）。送り手はメッセージBとメッセージCを受け取り者へ送る。受け取り者は公開鍵システムの自分の秘密鍵（S）を使ってメッセージCを解読する。解読された文は共通鍵（K）である。受け取り者以外の秘密鍵では解読できない。受け取り者は共通鍵（K）を用いて共通鍵アルゴリズムによりメッセージBを解読し、平文を得ることができる。最初に共通鍵アルゴリズムを用いて、暗号化している理由は、共通鍵暗号化システムの暗号化スピードが公開鍵暗号化システムのスピードに比べ一万倍速いためである。共通鍵（K）を公開鍵で暗号化することにより、公開鍵暗号化システムのメリットを活かしながら、秘密鍵暗号化アルゴリズムのスピードを確保できるというハイブリッド方式である。公開鍵暗号化システムのメリットは鍵の数がユーザ数（N人×2個分／人＝2N）個ですむという点にある。共通鍵暗号化システムでは、秘密鍵の数が交信するユーザの組み合わせ分（N×(N－1)／2）個必要ということになり、鍵の管理が個人の大きな負担になり、大規模な利用者の組織では使用できない。

5．システムのアーキテクチャー

システムのアーキテクチャーに対するセキュリティポリシーとして次のような事項がある。

（1）リモートアクセス

セキュリティの高いシステムでは1タイムパスワード（伝送路上を流れるパスワードが毎回異なる方式）を採用しないといけない。電話によるネットワークへの接続はネットワーク管理者と情報セキュリティ管理者の承認が必要。セキュリティの低いシステムではパスワードを定期的に変えることを義務づけ、電話によるネットワーク接続はネットワーク管理者の承認が必要。住友化学が採用しているRAS／DSSは1タイムパスワードを採用している。

（2）社内のデータベースへの外部からのアクセス

セキュリティの高いシステムでは、外部からの社内のデータベースへのアクセスは禁止。

どうしても外部からのアクセスが必要な場合は、外部向けにファイアーウォールの外にデータベースサーバを設置する。セキュリティの低いシステムでは、外部からの社内のデータベースへのアクセスはファイアーウォール上のプロキシー（アクセスの代理人）を介してのみ許す。プロキシーはネットワーク管理者が設定する。住友化学の場合は現在は社外からのアクセスはアクセスサーバを限定し、内部の特定サーバのみアクセス可能にしている。

（3）複数のファイアーウォールの設置

セキュリティの高いシステムでは複数のファイアーウォールは同一のもので構成されるべきであり、管理も1人のファイアーウォール管理者によってなされなければならないと言われている。Confidentialを含む重要なデータベースはファイアーウォールで外部からのアクセスを禁止すべきである。住友化学のSCNETの場合は住友化学と4社のグループ会社がインターネットのアクセスポイントを持っている点もあり、同一機種、1人の管理者は今後の課題である。

6．インシデントへの対応

コンピュータ、ネットワークへのインシデント（事故、緊急事態）への対応について。

（1）侵入の検出

侵入検出の支援機能は2つある。ひとつは現状の弱点をセキュリティ管理者に教えることにより、他のセキュリティシステムの導入等を促す機能である。もうひとつは障害に対する対応を始めるタイミング、トリガーを与える機能である。

（2）侵入検出の方法

侵入検出の方法としては大きくわけて2つある。ひとつはユーザからの苦情、問題点の指摘を待つ方法、もうひとつは監査用のログの監視する方法がある。ファイルシステムが不正に変更されてないことをモニターするツールも有効である。またファイアーウォール、ウイルスチェックソフト等は攻撃あるいはウイルスの侵入を受けたことを検知した時にネットワーク管理者へメールが行く仕組みになっている。またネットワークトラフィックのリアルタイムモニターでネットワークトラフィックの異常を検出する方法もある。セキュリティの高いシステムでは、全てのホストコンピュータ、サーバにロギング機能を実装する必要がある。ファイアーウォール、ウイルスチェックソフト、リモートアクセスサーバに上記の警報機能も装備する必要がある。全ての重要なサーバにはタイプの異なる侵入検知システムを2種類搭載する。

（3）インシデントへの対応

障害、緊急事態発生時の対応について文書で明確に整理しておく必要がある。その文書に従い冷静に事故に対応する。文書には下記のような点を記載しておく必要がある。

事故への対応行動を決定する人は誰か、いつ法的

な対応を取るか、侵入を直ちに止めるのか、あるいは当面侵入を許しながら、攻撃方法の詳細解明に努めるのか。

7．ネットワーク等の管理

技術的な問題とは別に管理面で下記の重要な項目がある。

（１）ネットワーク管理者への権限付与

ネットワーク管理者の選任は十分な調査を行い、適任者を選ぶ必要がある。特に新規採用者にいきなりネットワーク管理者の権限を全て与えるのでなく、その人の仕事振りを見ながら徐々に権限を広げて行く必要がある。

（２）適切な利用

インターネットあるいはWWWの適切な利用についてポリシーを定める必要がある。セキュリティの高いシステムでは、認められたユーザのみがインターネットへの任意のアクセスを認められる。一般ユーザは別のアクセスサーバを経由し、限定されたインターネットサーバしかアクセスできない。セキュリティの低いシステムではインターネットの有用性を会社が高く評価しており、その活用を薦めている。その場合の制約は、私用にインターネットを利用してはいけない。家庭に置いた会社のPCからインターネットの利用も許すが、社内の重要情報を社外へ送ることは禁止。

住友化学は社外のWWWの利用に関しては、セキュリティの設定は低いほうである。

（３）プライバシーの保護

個人が利用しているメール、ホームページの監視等は会社の情報保護の為にのみに限定し、それ以外の目的では、これらの情報を監視することはしない。

8．リテラシーとセキュリティ教育

利用者に対するセキュリティ教育はきわめて重要であり、また効果が高い。例を挙げれば、パスワードを定期的に変える（現実はそれ以前の問題として、最初にシステム側で用意したパスワードを変えていない人もかなりいる）、パスワードをPC等の傍にメモしない、パスワードを他人に教えない。ウイルスに汚染する可能性がある家族が使用するパソコンからは会社のネットワークへアクセスしない。不要な大容量のファイルを添付したメールを多数の人に出さない。ログオンしたまま長時間席を外さない、席を外す場合は、必ずログアウトする。現在住友化学へ導入中のExchangeの場合、ネットワークログオン（住化ドメインにログオン）していれば、他人がクライアントソフトであるoutlookを起動することでそのPCの持ち主のメールを読んでしまう危険があるので利用者への教育を徹底している。

セキュリティに関する国際標準の動き

1．ISO15408（セキュリティ評価認証制度）の紹介

個々の情報処理製品（データベース、ファイアーウォール、ICカード等）や情報処理システム（インターネットバンキング、認証サービスなど）のセキュリティ完備状況を評価し、認証するための国際標準が1999年6月にISO15408で定められた。ISO15408[7]の基本的な考え方は「製品やシステムの開発・製造・運用にかかわった資材を検査することによって、大丈夫であることを確認する」というものである。

検査の対象となるのは、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、テスト文書、マニュアル、開発者・業務者への教育・業務規約など通常の開発や運用で作成するものである。これらに加えてセキュリティ固有の生産物であるセキュリティ基本設計書と脆弱性分析書も含まれる。

2．国際標準化の目的

セキュリティについての最低の要件を定め、ここまでは全員が対策をしようという国際的な申し合わせである。

① どこまで企業秘密を管理すれば秘密として管理したことになるか

② どこまでプライバシー情報を管理すれば社会的な責任を果たしていることになるか

ということについて、国際的な標準が定められた。

3．ISO15408の仕組み

ISO15408は大きく分けて「機能要件」と「保証要件」とに分かれる。機能要件はシステムが有するセキュリティについての機能のこと。保証要件はシステムの品質に関する要件である。セキュリティ評価基準に適合しているときは「認証」が行われ、「証明書」が発行される。

4．ISO15408の特徴

① セキュリティ対策はセキュリティの脅威に対し有効な手段を提供するものを採用すべきであることを明確にした。むやみにセキュリティを高くすることを要求せず、必要なセキュリティ対策の実施を要求した。システム設計の段階で、セキュリティの脅威の分析と最適な対策のためのアプローチ方法を規定している。そのために「セキュリティ基

本設計書」の中でセキュリティの脅威の分析とその対策の策定、その十分性の検証を行う。以降のシステム開発はすべてこの規定内容に従う。

② システムの利用環境に応じて、自由にセキュリティレベルを設定できる。

具体的には7つのレベルから最適なレベルを選択できる。これを保証レベル（AEL：Assurance Evaluation Level）と呼んでいる。

③ 実施されているセキュリティ対策の内容の透明性を高めている。セキュリティに関する言葉の定義を行い、セキュリティ対策の推奨モデルをこの共通の言葉で規定することにより、設計者も利用者もセキュリティ対策に関して共通の理解を得ることができる。

5．ISO15408のビジネスへの影響

今後は、ISO15408の制定により、システムの構築や運用において、国際的な規模で種々の影響が出てくることが予想される。システムの利用者に対して、当該システムが安全であることを証明する方法として、利用者側からこの基準に基づく評価・認証を取得していることが要求されるようになる。国際標準であるから、この認証を取れば、海外でもセキュリティでもセキュリティの基準に適合していることが認められることになる。製品を輸出する場合のみ必要になるのではなく、今後企業間ネットワークを構築していく上で、自社が使用している製品・システムがISO15408に適合していることが、相互接続を認められる条件になる。ネットワーク接続できないことは企業間の取引ができなくなることを意味し、経営上の大きな問題となる。

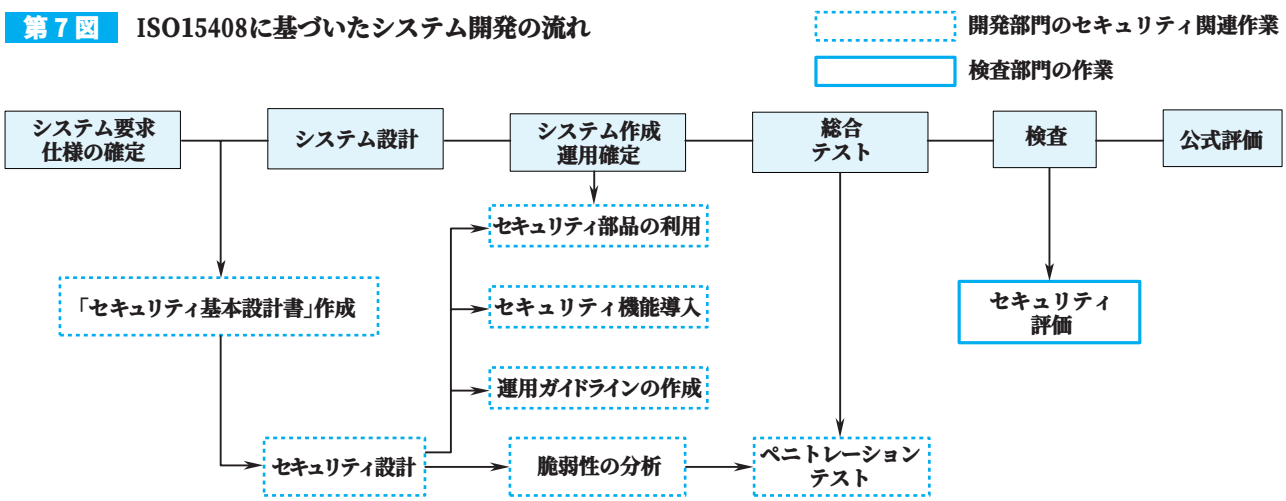
6．ISO15408基づいたシステム開発の流れ

第7図にISO15408に基づいたシステム開発の流れを示す。

住化グループにおける情報セキュリティ確保に向けての今後の課題

住友化学はセキュリティポリシーを既に定めており、今後はグループ会社のセキュリティポリシー設定を支援する必要がある。住化グループ会社各社はネットワーク及び各種サーバを共有することにより、経済性、利便性において大きなメリットを享受している。反面セキュリティ面では、セキュリティの低い方に全体のセキュリティレベルは引き下げられる危険があり、一定のセキュリティレベルを全体で確保する必要がある。セキュリティ対策は始まったばかりと言っても良い段階であり、より高いレベルのセキュリティの確保にむけてこれから為すべき課題は多い。本文は社外からの脅威を中心に述べたが、米国ではネットワーク犯罪の6割から8割は会社内部者の犯行といわれており、社内向けセキュリティ対策の実施を今後強化する必要がある。事業所間のアクセス制御やメールデータの永久保存等はその対策の一例である。認証に関してはECへの対応を含め、世の中の標準に合わせた認証システムの導入を検討している。またイントラネット等複数サーバへアクセスを一度のログオンで可能にするシングルサインオンの導入により、ユーザの利便性を確保しながらセキュリティレベルを上げる方法も今後の検討課題の1つである。現在導入中のERP、Exchangeが要求するネットワーク能力を保証するために、ネットワークトラフィックの測定と予測を行い、適切なネットワークの増強を図る予定である。安定した運用を行うためにセキュリティガイドライン、各種の運用基準の整備に努めている。技術の進歩が激しいので、外部の技術力を活用しながら、セキュリティホールへの対策、監査ツールの導入、そして定期的な監査の実施を行い、ネットワーク、サーバ、PC、セキュリティ管理者及び利用者を対象にしてシステム全体のセキュリティの向上を図っている。

第7図 ISO15408に基づいたシステム開発の流れ



引用文献

1) 日新電機株式会社情報通信開発事業部：ネットワークセキュリティ－脅威とその対策－
2) Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt：コンピュータセキュリティハンドブック（1995）
3) Internet Security Policy：A TECHNICAL GUIDE：National Institute of Standard and Technology Gaithersburg, MD 20899-0001 November 14, 1999
4) C. C. Wood：Information Security policies Made Easy Version7（1999）
5) 株式会社インターネットイニシアティブ　歌代和正：インターネット上での安全性の確保（1999）
6) 富士通株式会社　大塚 英夫：EC(電子取引)の現状と展望（1999）
7) セキュリティ評価基準の活用とセキュリティポリシー作成マニュアル（社団法人日本情報システムユーザ協会）（1999）

PROFILE

雪浦　和雄
Kazuo Yukiura
住友化学システムサービス株式会社
システムセンター
次長，技術士(情報処理部門)