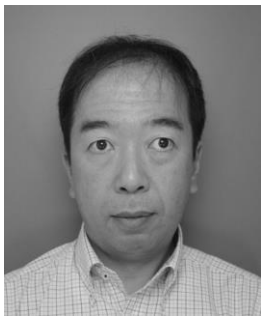
情報システム・サービスにおける IT セキュリティ管理策の適切な選択と実施に関する考察

システムライフサイクルにおけるセキュリティ実践



コンサルティング推進部
セキュリティプロフェッショナル

中村　一成

Kazunari Nakamura

kazunari-nakamura@exa-corp.co.jp

昨今、機密情報漏えいや個人情報にかかわる重大な事故などが頻発し、情報システム・サービスに対しても対策とともに管理水準の向上が社会的に求められている。これを受けて法令・公的ガイドラインにより組織に対し情報の管理責任が問われるようになり、システム開発やサービス提供の面ではコンプライアンス遵守の必要性が増している。本論文では現状を整理し、システム・サービスのライフサイクルにおけるセキュリティ管理のベストプラクティスについて考察する。

1. はじめに

情報システム・サービスでのセキュリティ確保が問われるようになって久しいが、システム設計や実装の不備、不適切な運用などによる情報漏えいが多数発生している。

また悪意の攻撃者の増加や攻撃手法の高度化で、場当たり的な対策では、もはや情報システム・サービスを適切に保護できない状況である。

セキュリティ事故発生時には、当事者個人だけではなく、組織として情報セキュリティの取り組みが問われることが増えている。その場合、システム的なセキュリティ機能の有無だけではなく、組織全体としてセキュリティ管理が行われ、その管理下でシステムに対するセキュリティ維持がされているかが問われる。

また、情報保護にかかわる法律や規格が年々強化されて、いっそうのセキュリティの強化が必要なことも明白である。さらにクラウドサービスの利用が普及し、ライフサイクル全般でのセキュリティの確保が複雑になってきている。

著者はセキュリティコンサルタントとしてさまざまな企業に情報セキュリティ改善・推進支援コンサルテーションを行ってきた。その際に、お客様のセキュリティ対策を確認すると、情報システムに対するいくつかのセキュリティ対策のみ考えていたり、セキュリティ対策の優劣を決めかねて検討が停滞していたりすることが見受けられる。この状況は個別のセキュリティ対策を積み上げる方法の限界であり、体系的にセキュリティに取り組まなければ組織が目標とするセキュリティの達成は困難であることを意味している。

組織的なセキュリティ管理は、セキュリティ管理のよりどころとなる組織ポリシー・ルール・手順の整備や、それに基づく判断・実施の記録整備などの組織的な取り組み、いわゆるマネジメントシステムの構築が必要になる。

システムに対するセキュリティ対策は、個別の情報システム・サービスが扱う情報、その情報にかかわる脅威の洗い出し、それぞれのリスクの大小を評価し、適切かつ現実的な管理策を選択しなければならない。

本論文では情報システム・サービスのセキュリティ改善を進めるうえでの、現実的な手法を述べる。以下、2 章では情報セキュリティ推進のよりどころとなる各種コンプライアンスの位置づけ、3 章では情報セキュリティ推進全体と IT セキュリティとの関係、4 章では具体的な IT セキュリティ管理策の適用、5 章ではセキュリティ管理策を継続的に運用するための組織的な管理について述べる。

2. 情報セキュリティコンプライアンス

コンプライアンスには法律、省令、法に基づくガイドライン、通達、公的規格(ISO/IEC,JIS など)、業界規格・ガイドラインなどがあるが、取り扱う情報や業務に対応したコンプライアンスから情報管理のありかたや組織的な取り組みが求められる。コンプライアンスは法令遵守と呼ばれることが多いが、法令だけではなく各種規格への適合や自社ルールの遵守を含んでおり、これらの要求から逸脱しないように運用しなければならない。

最も重要なコンプライアンスは不正競争防止法である。この法律で示される営業秘密とはビジネス活動にかかわる秘密性のある情報であるため、業務やシステムで扱う情報のほとんどが管理対象となる。

次に重要なコンプライアンスは ISMS(Information Security Management System、情報セキュリティマネジメントシステム）ISO 27000 シリーズである。情報セキュリティ管理の規格で、情報セキュリティ活動はこの規格の枠組みを活用して整備していくことが多い。

ほとんどの情報システム・サービスでは人にかかわる情報を扱うため、先の２つに加えて個人情報保護法も重要なコンプライアンスである。

2.1. 不正競争防止法と営業秘密管理指針

法律条文は抽象的でわかりにくいため、情報セキュリティにかかわる部分を実際の判例などを交えたガイドラインが営業秘密管理指針である。これをセキュリティ対策の具体的なよりどころとすることが多い。

不正競争防止法では営業秘密の漏えいなどを行った者に刑事罰や賠償責任を負わせているが、法的保護を受けるには、客観的にみて情報を秘密として管理していることが必要である。これは秘密管理性と呼ばれる。

紙文書では機密区分表示と施錠管理の実施、電子データではアクセス権限管理を実施し、かつ利用者には情報の秘密性を認識させなければならない。管理が有名無実化した場合に法的保護を受けらなかった判例が出ているため、対策の確実な実施が重要である。

2.2. ISMS(ISO 27000/JIS Q.27000 シリーズ)

情報セキュリティ管理の国際規格が ISMS である。ISMS では情報セキュリティに関する組織的な管理の枠組みや実施すべきセキュリティ管理策を示している。注意点として、各管理策では管理項目を示しているが、達成すべきセキュリティ水準は示していない。このため、各種法令・ガイドライン・規格をベースラインとして参照し、システムの特性や業務上のリスクに応じてセキュリティ水準を定めなければならない。

他のコンプライアンスではISMSの確立を前提していることが多い。したがって、ISMS 認定取得のいかんによらず、ISMS の考え方にのっとったセキュリティ推進が重要である。

2.3. 個人情報保護法、経済産業分野ガイドライン、JIS Q.15001

個人情報保護法は、個人情報の適正な管理に関する法律である。原則、個人情報の利用目的を明示し、個人情報取得対象者（本人）の明確な同意を得て取得し、目的の範囲内で利用しなければならない。

個人情報の取扱いにかかわる昨今の状況を素早く反映させるために、各監督官庁より業種別に管理策を具体化したガイドラインが示されている。なかでも経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」、通称 経済産業分野ガイドラインをよりどころとする場合が多い。このガイドラインは各分野に共通する事項が多く、最新の状況を反映して頻繁に更新されているため重要である。他省庁からのガイドラインはこのガイドラインに業種別の事情を反映ないし強化している。取り扱う情報の種類や顧客の監督官庁から該当するガイドラインを確認し、必要な個人情報管理策を実施することが重要である。

当初の目的を超えた個人情報の利用は、再度本人の同意が必要で無断転用は違法である。システムでは登録済みの個人情報を別の目的に利用する場合、個別に本人の同意を得るオプトインを経て再利用しなければならない。

個人情報は6か月を越えて保有すると「保有個人データ」となり、保有者に開示、訂正などの要求に対応する責任が発生する。システムや業務ではこれらに対応できるような機能を組み込んでおく必要がある。業務上の必要性が少ないのであれば、取得後6か月以内の消去が望ましい。

最近は、個人を明確に特定できる情報だけではなく、クレジットカード番号、監視カメラ画像、位置情報、携帯端末固有番号など個人に強くひもづく情報はプライバシー侵害のリスクが高まっている。そのため、これらはパーソナル情報として個人情報と同等の管理が求められようになってきている。

組織として個人情報保護の取り組みはマネジメントシステム規格の JIS Q.15001 に示されている。したがって、P マーク認定取得にかかわらずJIS Q.15001にのっとることが望ましい。

2.4. 関連コンプライアンスの認識

不正競争防止法や個人情報保護法だけではなく、システムが扱う情報の内容やサービスが対象とする業務によって、さまざまな法令や規格などのコンプライアンスが影響する。このため、専門家の助言を受けたうえで、その分野の関連法令や規格が何か、優先するものを理解し、適切な対応を行うことが重要である。次の表.1に代表的な法令・規格などの関連コンプライアンスを例示する。

表. 1 代表的な関連コンプライアンス

法令・規格	概要
不正競争防止法、営業秘密管理指針、ISMS	情報保護全般に関する要求事項、管理の枠組み
著作権法、商標法	Web コンテンツ全般
個人情報保護法、経済産業分野ガイドライン	個人情報の定義、管理義務、利用目的の明示、同意を得た取得、保護対策例
不正アクセス禁止法	システムの管理責任
プロバイダ責任制限法	トラブル対応や情報開示責任
割賦販売法、PCIDSS	クレジットカード番号の保護
特定電子メール法	メールマガジンやDMの発行など
特定商取引法	通信販売にかかわる表示義務
景品表示法	キャンペーン実施にかかわる表示義務、抽選の公平性
金融商品取引法、J-SOX、	経理・会計を中心とした財務報告の正確性確保

関税法	輸出入にかかわる電子メールなどの保管義務

IaaS・SaaS 等クラウドサービスは日本国外からサービスが提供される場合、提供国の法令についても意識しなければならない。

システムインテグレータの立場では、システムや業務にかかわるコンプライアンスが何であるかを自発的に確認し、顧客に対して注意喚起・提言を行い、コンプライアンスを遵守した安全な情報システム・サービスを実現することが重要である。

3. 情報セキュリティへの取り組み

セキュリティ改善に取り組む際、個別の対策から考えることが多くみられるが、保護しなければならない情報資産、情報資産に対する脅威、および脅威によるリスクが何かを踏まえて、リスクを減らす適切な対策を考えることが重要である。また、対策の効果・費用・利便性のバランスが重要である。

コンプライアンスからのセキュリティ対策は必須だが、それだけでは不十分な場合も多い。特にインターネットシステムでは定常的に攻撃にさらされるうえに、新たな攻撃手法が出現する高いリスクにさらされている。また、クレジットカード情報や健康情報など取扱いに細心の注意が必要な情報はその取扱い自体に高いリスクがある。重要な情報資産を扱うシステムや、インターネットの脅威にさらされるシステムでは、ビジネスとしてこのリスクレベルを理解し、受容できるかを判断しなければならない。

リスク分析はシステムやサービスが扱う情報資産に対し網羅的にリスク評価を行い、セキュリティ対策は高いリスクから実施していくのが、バランスのとれたリスク対策となる。なお、一般的なリスクマネジメント手法は ISO31000 を参照していただきたい。

3.1. IT セキュリティの定義

ISMS では情報が記録・保管されている情報資産を保護対象として管理する。情報資産には情報システム・サービスの他、電子媒体、紙文書、構造自体に秘密性がある機械・設備などの化体物も対象になる。

ISMS では情報資産に関するセキュリティリスクを低減する対策を管理策(Control)と呼んでいる。管理策はシステムで実装するセキュリティ機構・機能に相当する技術的管理策の他、設置場所・保管場所などの管理などの物理的管理策、システムの利用者やシステム管理者に対する教育や確認などの人的管理策、これらを PDCA で管理する組織的管理策がある。これらの管理策を組合せでセキュリティリスクを一定以下に保つという考え方である。

システムでのセキュリティ対策は効果が確実だが導入・運用コストがかかることが多い。人によるセキュリティ対策は教育コストのみで済むこともあるが、実施に高いスキルを必要とし、また徹底や確認が困難な場合がある。効果が期待でき合理的な実施が可能な管理策を IT、人、物理でバランスよく実施することが望ましい。

セキュリティ管理策のうち、情報システム・サービスでの情報資産の管理については、情報システム・サービスにかかわる物理的管理、IT サービスの利用者および運用者に対する人的管理、IT 部門での組織的管理など IT に強くかかわる部分は IT セキュリティ管理とする。

3.2. IT セキュリティの整備にあたって

情報システム・サービスに対するセキュリティ管理策は、組織の情報セキュリティポリシー体系を構成する IT セキュリティポリシーから導かれることが望ましい。

しかし、情報セキュリティポリシーは整備中だったり、ポリシーが抽象性の高い記述にとどまりとどまったりして、セキュリティ要件として用いることが難しいことがある。

このような場合、情報セキュリティポリシーの整備を待たずに、法令・規格などのコンプライアンスをよりどころとして、先に IT セキュリティポリシーを整備することが効果的である。

関係する法令・ガイドライン、公的・業界規格などから IT にかかわる管理方針や要求事項を IT セキュリティポリシーとしてまとめ、個別のシステム・サービスに対する IT セキュリティ要求・要件に用いることができる。

各コンプライアンスでの IT に対するセキュリティ要求はかなり重複しているため、共通の管理策にまとめることが多い。

情報セキュリティポリシーの整備を後回しにしても、共通コンプライアンスをよりどころとしているため、ポリシー間の整合性確保は可能である。

IT セキュリティ管理策は、システム・サービス上にセキュリティ機能として実装するものと、システム運用で実施するものに大きく分かれる。セキュリティ機能の実装はコ

ストが必要であり、概算費用算出や非機能要件定義などのシステム開発の早い時期にセキュリティ機能の必要性を認識しなければならない。システム化を急ぐ場合には、IT セキュリティポリシーは実装ポリシーから整備し、要件定義などに用いる場合もある。

個別システムでは、自組織のセキュリティ要求水準に加え、取り扱う情報に関する法律や規格などのコンプライアンス、システム固有の脅威などを考慮したセキュリティ管理策が必要である。

4. IT セキュリティ管理策とその実装

セキュリティ管理策として、システムにセキュリティ機能を実装しても、運用に不備があればセキュリティリスクは増大してしまう。特にソフトウェアにかかわる脆弱性は必ず新たなものが発生するため、継続的な対策を行わなければリスクは増大する。システム利用者は入れ替わるため ID やパスワードは適切に管理しなければ、不正アクセスのリスクが増大してしまう。

実施すべきセキュリティ対策はいくつもの選択肢があるが、存在する大きなリスクを効果的に低減できる対策から着実に実施し、システム全体のセキュリティを向上させていくのが適切である。

以下、分野別の取り組みを示す。

4.1. IT 資産管理

組織の IT セキュリティ推進の第一歩は、各情報システムのセキュリティ状況を把握することである。このため IT 資産管理から取り組むことが多い。

IT 資産管理では固定資産情報だけではなく、システム構成、ネットワーク構成、セキュリティに影響を及ぼす導入されているソフトウェア群、主たるデータベースやファイルなどの取扱い情報資産なども管理することが望ましい。代表的な管理項目を表.2 に示す。

表.2　代表的な IT 資産管理項目

管理項目	項目例
体制	ユーザ部門責任者(所有者)、システム管理者
概要	システム名称 システムの機能(業務アプリ、ファイルサーバ、インターネット Web など)
	利用者 ID 数(社内、社外)、管理者 ID 数
取扱情報	種別(自社秘密、他社秘密、消費者個人情報、機微情報など)、件数、保管期間
ハードウェア	設置場所、機種、ストレージ容量、保守窓口、サポート期間など
ソフトウェア	OS,ミドルウェアのバージョン・パッチレベル管理、ライセンス番号
ネットワーク	回線種別、帯域、構成
システム文書	設計書、設定シート、ソースコード、運用手順書、運用体制図、作業計画書・実施記録
外部サービス	通信回線契約、クラウド・ASP などサービス契約、業務委託契約

特にソフトウェアについては、脆弱性発見に伴うパッチ・バージョンアップの必要性判断や、サポート契約管理などの基礎情報となるため、システムライフサイクル全般で最新性が維持できるような管理を想定しておかなければならない。

4.2. 利用者識別・認証機能

多くのシステムでは正規の利用者かどうかは、ID・パスワードを用いログイン画面で利用者の識別・認証を行っている、この機能はセキュリティ管理上極めて重要であるが、多くの脅威にさらされている。

インターネットシステムでは、識別・認証機能への攻撃を行う自動ツールも存在し、日常的な攻撃を前提とした対策が必要である。総当たりや辞書式のパスワード攻撃手法には、認証失敗のたびに次の認証までの時間を次第に延ばすことや、一定回数以上の失敗でその ID や送信元 IP アドレスからの認証を受け付けないロックアウト機能も有効である。

フィッシング詐欺では偽サイトで ID・パスワードを盗み、EC サイトなどの正規サイトで不正購入すること手法がある。対策には通常と異なる端末からのアクセスを Cookie 情報、ブラウザ種別、IP アドレスなどから識別し、疑いがある場合には二次認証情報を求めることが有効である。

識別・認証機能では、入力された ID と認証の成否、ログアウトやセッション切断などの事象を時刻とともに記録しておくことが必要である。この記録は正アクセス発生時の遡及に用いるとともに、不正なアクセスがないことの証

跡となるので重要である。

4.3. 利用者管理

識別・認証機能は、利用者が用いる ID・パスワードなどの適切な管理を前提にしているが、現実には管理の不備や改善すべき点が多い。

ID 管理では、利用者の退職・職務変更の際に、利用者削除や無効化が行われていない場合がある。パスワード管理では ID と同じパスワードの設定、予測可能な単語、長期未更新によるパスワード推定リスクがある。

社外取引先や業務委託先にシステムを利用させている場合、１社に１ID の運用が多い。この場合、複数人での ID 共用や、担当者変更時に ID・パスワードを引き継いでいることがある。共用 ID の利用は事故発生時の個人特定を困難にし、インターネットシステムでは退職者・離任者などによるアクセスが可能など、高いリスクがある。１ユーザ・１ID を徹底し、定期的なパスワード更新が望まれる。１社１ID の運用を継続せざるを得ない場合は、担当者変更時はパスワード変更を徹底し、抜本的な対策までの代替策とすることもある。

パスワード忘れや期限切れに際し、パスワード再発行を行うが、これを悪用し不正にパスワードを奪取しようとするソーシャルエンジニアリングのリスクを意識しなければならない。再発行では確実な本人確認手順が必要となる。

情報システムにはすべての利用者 ID とパスワード情報が保管されているため、この情報の漏えいリスクの考慮が必要である。パスワードの平文保存は漏えい時に他サイトへの攻撃に用いられ、二次被害が発生する場合がある。パスワードの平文保存は避けるべきで、復号不能なハッシュ関数を用いた不読化が望ましい。パスワードの復号が必要な場合は暗号化するが、万が一パスワードファイルが漏えいした場合でも、暗号化鍵と同時に漏えいしない対策が必要である。

管理業務は ID 発行から廃止までの流れが複雑で例外も多いため、業務全体のリスク分析を行い適切な対策を検討すべきである。管理負荷削減の面からは、システム別の利用者管理は避け、組織共通の ID 管理・認証基盤の活用が効果的である。

4.4. アクセス管理

アクセス管理は狭義にはネットワーク層での通信制御を指すことが多い。具体的にはファイヤーウォール、サーバ種別ごとの LAN 配置、各サーバでの IP アドレス通信制限や通信記録の取得などが該当する。通信制御はファイヤーウォールで一括実施する場合や、iptables, ipfilter などのサーバ側での個別実施する場合など、さまざまな方法があるが、同一 LAN 内システムは同一セキュリティ水準とすることが望ましい。これは同一の設定を展開できるため運用が効率的になることだけではなく、第三者による点検や監査でセキュリティ機能が有効であることを示しやすい点も挙げられる。逆にセキュリティ水準が異なるシステムや用途・目的が異なるシステムを同一 LAN に混在させるべきではない。

インターネット系システムでは、日常的にさまざまな攻撃を受けるため必要な通信のみを透過させるための FireWall の設置が一般的であるが、透過させた必要な通信に対してもさまざまな攻撃が発生している。必要な通信にかかわる攻撃を遮断するためには IPS・WAF などの機器を活用し、多層防御することが望ましい。

4.5. 権限管理

利用者がファイルやデータベースに対して追加・閲覧・更新・削除などの操作可否を管理するのが権限管理である。Need to Know の原則で、業務上必要な操作のみ可能とするように利用者に権限付与しなければならない。

権限付与は個人や部署を単位として行うが、ファイルサーバではアクセスできる全員がデータを操作できる状態が見つかることがある。アクセス権限を部門に任せている場合に、他部門にアクセスさせるために権限を変更しているうちに、業務上必要な範囲を超えた開示範囲になっている場合がある。

このような状況は秘密管理性があるとはいえず、悪意による情報漏えいが起きた場合に、不正競争防止法による法的保護が受けられない可能性がある。

権限管理は、現実的な情報保護効果が発揮されるような運用が重要である。

4.6. システム特権管理

情報システムそのものに大きな変更を加えることのできるシステム ID やその権限の管理はシステム特権管理として、通常の利用者 ID 管理・権限管理とは別扱いする。OS の特権には Linux/UNIX における root や Windows におけ

る Administrator などがある。データベース管理者(DBA)の ID もシステム特権として扱われる。

特権管理が注目されるのは、重大な情報セキュリティ犯罪・事故はシステムに近い者が関与することが増え、各種コンプライアンスからシステム特権に対し厳密な管理が求められている。

システム管理者による特権作業は、承認に基づく正しい作業のみを行っていることが原則で、これを客観的に示すことが必要である。最低限、システム管理者による作業内容、作業日時を記録し、定期的に不正が行われていないことの確認が重要である。事故発生時には記録から該当する作業者、作業内容、日時の遡及が必要である。

特権 ID 保有者が異動・退職などで業務から離脱した場合は、即時権限を剥奪することなど、厳密な管理が必要である。

特権 ID にはシステム間通信で用いる ID があるが、通常の管理者 ID のような定期的なパスワード変更が困難な場合がある。この場合、通信用 ID での可能な操作を限定し、電子証明書などの強固な認証方式を用いる。

ネットワーク機器などではシステムの仕様上、特権 ID を共有せざるを得ない場合があり、この場合、踏み台サーバを設置し、作業者 ID でログインし、目的の機器に対して作業を行う。この場合、作業者と作業内容を特定できるように、すべての作業記録を保存し、証跡とすることが重要である。

4.7. ログ管理

他のシステムから漏えいした ID・パスワードリストを用い、攻撃対象サイトへ不正侵入を試みるアカウントリスト型攻撃が増加している。対象サイトの利用者が漏えいしたシステムと同じ ID・パスワードを用いていた場合は容易に不正侵入を許してしまう。この攻撃は機械的に ID・パスワードを入力しアクセスを試みているため、多頻度の認証失敗や特定 IP アドレスからのアクセスがログに記録される。

現実にはログを取得していても、定常的な監視が不十分であることが多いが、インターネットシステムではアクセスや認証の事象を記録し、通常と異なる状況がないかを監視すべきである。

前述の識別・認証管理や権限管理機能による記録は、権限外操作だけではなく、権限を有する者が悪意で情報漏えいや改ざんを行う可能性を考慮すべきある。このような操作の遡及には成功・失敗双方の事象に関し、操作時間、操作者 ID、アクセス元 IP アドレス、データに対する操作など行為者と行為が特定可能な記録が必要である。

システムに対する監査では、情報システム業務が正しく実施されていることを確認するために、システム作業に対応した特権作業ログの提示を求められる場合がある。したがって、特権作業ログは監査証跡として改ざんや消去されないように適切な保護が必要である。ログ保護のためにログ保管サーバを設置し、各システムログはログ保管サーバに速やかに転送するとともに、独立したログ管理者を設けることが効果的である。

4.8. 暗号化と鍵管理

ストレージ上のデータや通信路の暗号化は容易になったが、適切に情報が保護できているかの検証が不十分なことがある。たとえば、データベースが暗号化されていても、認証や権限設定が不十分で、データへのアクセスが可能では暗号化の効果はない。

暗号化の暗号鍵が漏えいしないように厳重な管理を行うが、暗号鍵が漏えいした場合を想定し、対策を検討しておく必要がある。インターネットサイト用の SSL 秘密鍵が漏えいすると偽サイトを立ち上げられる可能性があるが、発生した場合は SSL 証明書を失効させる対策がある。一方、証明書の有効期限があるため、定期的な暗号鍵と証明書の更新は重要である。

VPN 装置などの通信機器では機器間で同じ鍵を使う共通鍵方式が用いられるが、鍵を配布時に漏えいしない手段を用いる必要がある。暗号は計算能力を投入すれば解読できる前提での管理が必要で、暗号鍵の定期的な更新を想定した運用手順とし、運用コストを確保しなければならない。

安全な暗号化方式は時とともに変わるため、専門家により評価された方式から選択する。日本国内向けであれば電子政府推奨暗号リスト、海外向けには NIST や NESSIE が定める方式などがある。

クレジットカード番号の保管は PCIDSS では暗号化ではなく復号不能な不読化を強く求めている。技術的には SHA-1 のような一方向関数による処理が適切である。

4.9. 不正プログラム対策

Web サイトを不正に書き換えて、アクセスしたユーザ PC へ不正プログラムを導入させる事例が頻出している。

Web サイトではこのような不正プログラムを発見し除去するアンチウイルス機能の導入が一般的になりつつある。このため Windows だけではなく、Web サイトとしてよく使われる Linux でも同様の対策が必要である。

コンテンツや各種アクセスログなどの改ざんの発見には、Tripwire などのファイル改ざん検知機能を用い、不正な更新が発生していないことを定期的に確認する。

4.10. 外部サービスの管理

外部サービスはインターネット接続や広域 Ethernet 接続などの通信サービスを指すことが多かったが、スパムメール除去サービスや地図情報サービスなどアプリケーションに近いクラウドサービスまでに範囲が拡大している。

クラウドサービスの業務利用は自社の情報を扱うため情報資産として管理対象であるが、利用者に認識されていないことが多く隠れたリスクとなっている。セキュリティポリシーではクラウドサービスは外部サービスとして管理対象であることを示し、IT 資産管理の枠組みで管理が必要である。

クラウドサービスは機能や低価格が注目されているが、サービス障害時の影響や、突然の API の変更による不具合発生や、クラウド事業からの撤退・倒産によるサービス終了などクラウド特有のリスクを考慮しなければならない。

インターネットシステムでは低コストと導入の容易さから IaaS を用いる場合が増えているが、サービス継続性を考慮しなければならない。SLA(Service Level Agreement)ではサービス停止時の金銭的補償に言及しているが、これはサービスが停止しないことの保証ではないことを認識しなければならない。リスク管理の一環として、サービスの一時停止、仕様・約款変更、終了の影響は可用性リスクとして評価が必要である。

クラウドサービスにかかわる評価手法は ENISA ガイドラインなどを参照し、事業継続性の他、ベンダロックインリスクなども考慮しておくべきである。

4.11. 脆弱性管理

インターネットシステムでは、システムを構成する OS・ミドルウェア・開発アプリケーションに関するセキュリティホールが発見されるため、新たな攻撃に狙われることが日常的である。システムの設定不備や ID・パスワード管理の不備など運用の問題が脆弱性となることも多い。

これらの脆弱性を解消するには、自システムに関する定期的な情報収集と影響と対策要否を判断し、必要であれば判断基準の見直しなどを行う体制が必要である。脆弱性対策が有効であることを客観的に示すために、脆弱性検査を定期的に実施し確認することが重要である。

セキュリティホールに対応する修正パッチが提供された場合、対象システムに影響がなければパッチを適用する必要はないが、これを判断できる力量と体制が必要である。現実にはセキュリティ情報の評価と判断には高度な知見が必要で人材の確保は困難であるため、パッチ全適用が人的コストを抑えられる可能性がある。これらの高度なセキュリティ運用が困難な場合、専門家に業務委託することを検討すべきである。

4.12. 可用性管理と完全性管理

システム停止、処理遅延などにより情報資産の利用が一時的にできなくなる状況は、可用性が損なわれた状態である。要因としてハードウェア障害、回線障害、作業失敗、災害などの他、DDoS (Distributed Denial of Service)攻撃による場合がある。通信販売サイトでの新発売時にアクセスが殺到し、サービス提供が中断したり、遅延が発生したりする状態が該当する。

データやシステムの損傷を伴う重大な故障や災害、不正アクセスによるシステム破壊・改ざんなどが完全性が失われた状態である。

いずれも発生する可能性のある脅威、その影響、および確率を想定しリスク分析を行ったうえで、適切な対策を行うことが必要である。対策としてはリスクが現実に発生しないための予防策とともに、発生した場合の回復手順が必要である。

冗長化は可用性を向上させる手段であるが、人為的ミスや天災に対しては効果がない。先の大震災では予備機含めて失われてしまった例があり、回復手順の明確化と検証が重要であることを示している。

処理遅延や反応悪化などの事象では、どのような状態を可用性が損なわれたとするかの判断基準が必要となる。Web サイトなどでは利用者が次第に増え、システム負荷が高まり過負荷となりサービスに影響が出る場合があるが、定期的なシステム負荷の計測とともに、必要な増強を事前に行っておくことが望ましい。総合的なサービス継続の検討は BCP(ISO 22301)の一環に含めるのもよい。

回復手段としてはバックアップ・リストアがあるが、データバックアップだけではなく、人為的ミス、故障、災害などによりデータが破損・消失したリスクを考慮し、このような状況からの復旧手順を用意しておくことが重要である。多くのシステムではバックアップはあるが、復旧手順が未整備、もしくは手順があっても訓練していないなど、リストアできない場合がある。

経理や決裁など財務情報に関係するシステムでは、システム管理者が不正にデータ閲覧や変更を行わないことの牽制できているかを問われることが増えてきている。特権管理では完全性管理を強化し、データの不正な改ざん、消去、破壊されないよう対策を行うことが必要である。財務情報にかかわるデータだけではなく、システムに関する ID/パスワード管理 DB、権限管理 DB、暗号鍵、電子証明書などの重要な設定ファイル、認証ログやファイル操作ログなどが管理対象となる。

5. IT セキュリティ管理策の運用

セキュリティ対策はシステムの企画、設計、構築、運用のライフサイクルにわたって、適切に取り組まなければならない。また、システムごとのセキュリティだけではなく、IT 部門としてもセキュリティへの取り組みも重要である。これらに関して、以下で述べる。

5.1. 組織的なセキュリティ管理

IT 部門での組織的なセキュリティ管理は、セキュリティポリシーの考え方や管理要件が実際のシステム実装・運用に反映していることと、ポリシーに基づいて IT 部門の業務が行われていることである。

セキュリティ管理の向上には、システム実装・運用にかかわる必要なルール、基準、手順書、体制表、承認フロー、各種記録などを整備し、属人性を排除した業務にしていくことが効果的である。監査においてシステムが対象になることは前述したが、セキュリティ対策が有効に機能していることと、組織として運用していることを重視される。

IT 部門のセキュリティ構築・運用を確実にするため、システムの企画・設計・開発・構築など各段階に携わる者に対するセキュリティ教育も重要である。これらの教育資料やコースの整備もセキュリティの重要なテーマである。

システム構築や運用などを業務委託している場合、委託業務が適正に行われていることを委託元として確認することが必要であるが、委託先の組織的なセキュリティ管理状況を評価することが有効である。

5.2. システムへの管理策の適用

セキュリティ対策はシステムの企画時は十分に検討しておくことが重要である。検討は実装するセキュリティ機能だけではなく、運用手順や運用コストを想定し、システムライフサイクルにわたってセキュリティの維持が可能かの検討が必要である。また、顧客にはセキュリティリスクの認識、セキュリティ対策の効果、構築時および運用時のコストを十分に理解してもらうことが重要である。

設計・構築段階では、セキュリティ機能を正しく実装するだけではなく、その過程を第三者に示せるように記録、承認していることが重要である。具体的にはセキュリティ実装方針、ルール、セキュリティ対策などが文書化され、これに基づいて設計やコーディングがなされ、適切にレビュー・承認した記録を残さなければならない。

プログラム開発段階では、開発部分にバッファーオーバーラン、SQL インジェクションなどの脆弱性発生しないように注意深く設計し、コーディングを行う必要がある。また開発過程で脆弱性を生じさせないためにカスタマイズは避け極力パッケージ機能を用いることや、脆弱性が入り込みづらい安全な開発フレームワークを採用するのも効果的である。

システム構築段階ではシステムに多数の設定を行うが、セキュリティにかかわる設定は全動作を許可しない Default deny とし、利用に必要な設定のみをしていくことが確実である。また、デフォルトパスワードの変更、不要 ID の削除、テスト用 ID の削除、テスト用データ、プログラムなどの削除なども重要である。

今までは、このようなシステム開発・設定手法を社内技術標準文書として整備することが多かったが、近年の攻撃手法の多様化や 0 デイ攻撃などの出現で内容の陳腐化が早くなった。このため、IPA の技術文書など最新の状況が反映され技術的な網羅性があり有識者による評価がなされた外部文書を活用することも増えてきた。

5.3. 標準化と効率化

セキュリティ対策を重視し過ぎると、運用が複雑化し高コストになる。これを避けるために IT セキュリティ対策

を標準化し、運用コストを低減する取り組みが必要である。

システムアーキテクチャの標準化はセキュリティ対策の評価、脆弱性情報の収集、パッチ適用判断、適用手順の整備などの負荷を低減するだけではなく、構築や運用の負荷、運用者に対する教育・点検などの負荷軽減も期待できる。より踏み込んで、多くのシステムで共通に必要な ID 管理・ログ管理・特権管理などを統合システムインフラとして用意し、各システムからはこれを活用する構成とすれば、セキュリティ向上・利便性向上・運用負荷低減の両立が可能になる。特に財務報告の正確性にかかわる J-SOX・SOX の活動では IT 全般統制を確実に実施する面で共通化・システム化が推奨されている。またシステム運用業務全体の標準化では ISO20000 や ITIL などの規格に準拠していくことが重要である。

6. まとめ

本論文では IT セキュリティに関する管理策について注意すべき点を示してきたが、実際のシステムにおいてはリスク評価に基づいて、適切な管理策を選択し実施すべきである。

リスク評価では、取り扱う情報資産を明らかにし、これら情報資産に対して考え得る脅威・脆弱性を列挙し、網羅的にリスクを洗い出す詳細リスク分析が重要である。詳細リスク分析は IT 面だけではなく業務全体の評価が必要で手間もかかるが、適切なリスク低減策を選択するには効果的で、分析の過程を通じて関係者間の認識が共有されるため、合意形成が進みやすい。

また、組織的なセキュリティ対策は IT 部門だけでは達成できないことが多く、関連部門との連携も必要で体制作りだけでも期間を要することが多い。このため短期間で実施可能なセキュリティ対策、時間を要するセキュリティ対策などを洗い出し、計画をたてて関係者と合意し、効果的な対策を着実に実施していくことが重要である。

本論文が IT セキュリティにかかわる問題に取り組むエンジニアの一助となれば幸いである。

参考文献

1) 経済産業省、営業秘密管理指針(平成 25 年改訂版)
2) 日本規格協会、情報技術-セキュリティ技術- 情報セキュリティマネジメントシステム－要求事項 (ISO/IEC 27001:2005)
3) 日本規格協会、情報技術-セキュリティ技術- 情報セキュリティ管理策の実践のための規範(ISO/IEC 27002:2005)
4) 日本規格協会、リスクマネジメント－原則及び指針 (JIS Q 31000:2010, ISO 31000:2009)
5) 経済産業省、個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成１６年１０月２２日厚生労働省経済産業省告示第４号 、平成２１年１０月９日改正）
6) 日本規格協会、個人情報保護マネジメントシステム－要求事項(JIS Q 15001:2006)
7) 経済産業省、システム管理基準 追補版（財務報告に係る IT 統制ガイダンス）
8) PCI Security Standards Council LLC,PCI DSS v2.0,
9) ENISA、「クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク」、「クラウドコンピューティング：情報セキュリティに関わる利点、リスクおよび推奨事項」
