特集論文

ISMSを利用した情報セキュリティ対策の要件定義

岩本　仁*
菅原和則*

Requirement Definition Method Using ISMS for Information Security Control

Hitoshi Iwamoto, Kazunori Sugahara

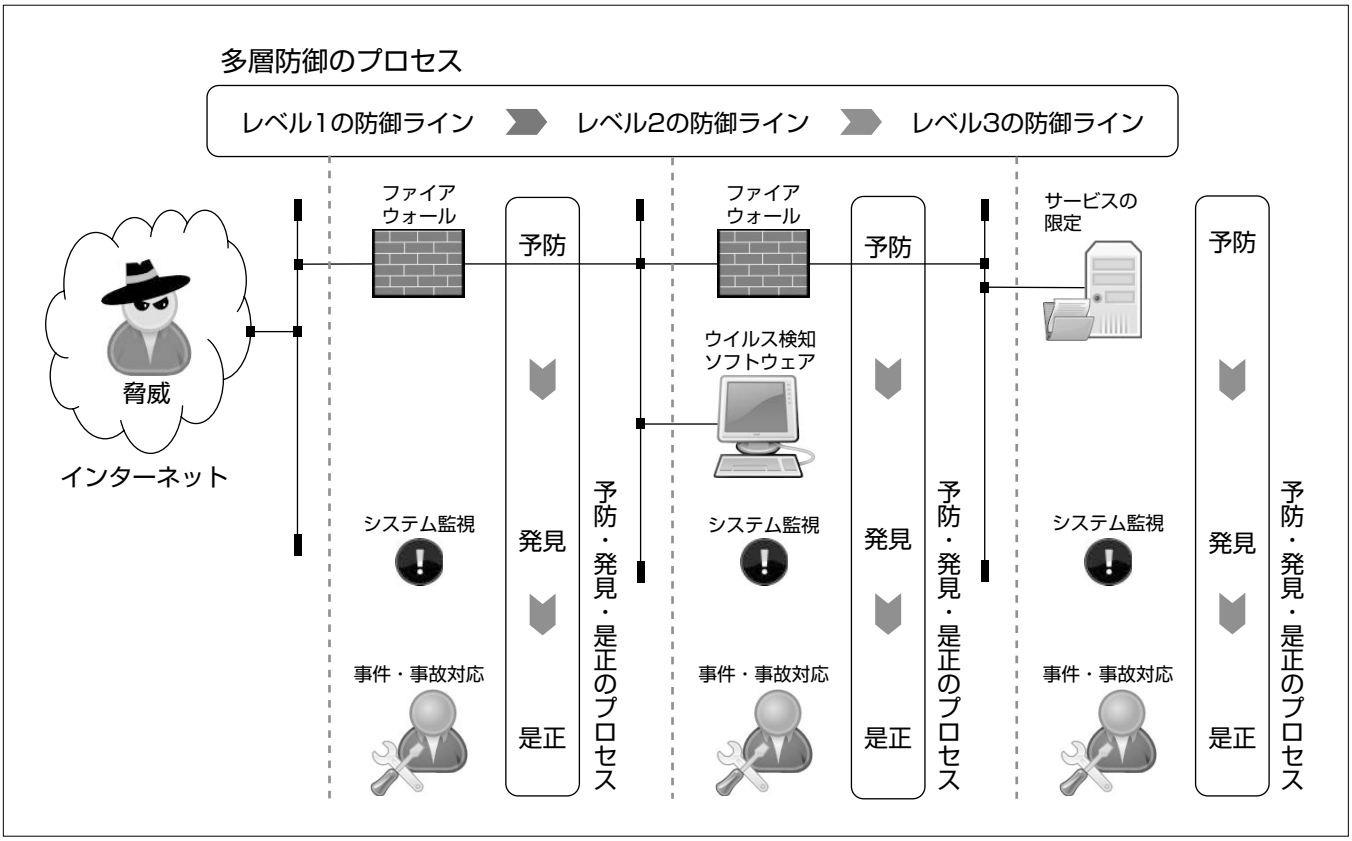
要　旨

情報セキュリティ対策とは，特定の製品のことではなく，脅威から情報を守るために個々の対策がつながって機能するプロセスである。情報セキュリティ製品や管理手順をプロセスとしてつなぎ，効果的な情報セキュリティ対策を構築するためには，情報セキュリティマネジメントシステム（Information Security Management System：ISMS）[(1)]が規定するリスクアセスメントを活用して，情報セキュリティ対策の要件定義を行うとよい。

リスクアセスメントでは，情報を狙う脅威の手口を分析し，次に対策の不備を見つける。そして不備を補うための対策をISMSの規定する133種類の選択肢から選ぶ。

選んだ対策は，プロセスとして機能するようにまとめ，情報セキュリティ対策の要件として定義する。プロセスには2種類ある。一つ目は，多層防御のプロセスで，守るものを中心にしてレベルごとに構築した防御ラインが順に機能することで脅威からの攻撃を防ぐ。二つ目は，予防・発見・是正のプロセスで，事件や事故が発生する前，発生したとき，発生した後の順に機能する。脅威からの攻撃を防ぎきれなかったときに，攻撃をいち早く発見し，被害の拡大を防ぎ，情報システムや業務を回復することができる。

本稿では，三菱電機インフォメーションシステムズ㈱（MDIS）がISMSの導入・維持のコンサルティングを通し，ISMSによるリスクアセスメントと他の技法を交えて行っている情報セキュリティ対策の要件定義方法について述べる。



プロセスとしての情報セキュリティ対策の例

多層防御のプロセスでは，レベル1の防御ラインで，外部から内部ネットワークへの通信をファイアウォールで制限する。レベル2では，二つ目のファイアウォールでサーバへの通信を制限し，パソコンにウイルス検知ソフトウェアを稼働させる。レベル3では，サーバで稼働するサービスを限定し，脆弱（ぜいじゃく）性を減らす。それぞれのレベルに，予防・発見・是正のプロセスがあり，予防できなかった攻撃をシステム監視によって発見し，事件・事故として対応し，被害の拡大を防ぎ，システムを回復する。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

MDISは，ISMSのコンサルティングを通して，効果的な情報セキュリティ対策を実現するため，リスクアセスメントを行って，個々の対策を実施の順序に統合したプロセスとして要件を定義してきた。本稿ではその手順の概要を述べる。

2. ISMSの特徴と利点

ISMSは，PDCA(Plan Do Check Action)サイクル，文書管理，経営陣の責任等といったマネジメントに関する点では，品質マネジメントシステム[2]や環境マネジメントシステム[3]と同じである。しかし，他のマネジメントシステムにはない特徴が二つある。一つ目は，どのような情報セキュリティ対策を実行するかをリスクアセスメントの結果に基づき決定する点であり，二つ目は，実行する情報セキュリティ対策を選択肢から選ぶ点である。

リスクアセスメントを行い，情報セキュリティ対策を選択肢から選ぶのには利点がある。リスクアセスメントで自組織内外の情報セキュリティに関する状況が把握できるので，対策の的が絞れて無駄が減らせる。一方，規格化された選択肢から対策を選べば，対策の漏れが減らせる。これがISMSの利点である。

3. リスクアセスメント

3.1 概　要

リスクアセスメントは，孫子のいう，“彼を知りて己を知れば，百戦してあやうからず”[4]に通ずる作業である。ISMSでは，“彼”のことを“脅威”，“己”のことを“脆弱性”と呼ぶ。脅威は，利害関係者に損害を与える何かであり，脆弱性は，脅威がつけこんでくる対策の不備である。脅威と脆弱性を知り対策を打てば，情報セキュリティも危うくなくなる。

ISMSが規定するリスクアセスメントの手順は，大きくまとめると次のようになる。

(1) 守るべき資産の特定
(2) 脅威が狙う脆弱性の特定
(3) 脆弱性対策の選定

このリスクアセスメントの手順に従って対策を選ぶ方法を次に述べる。

3.2 守るべき資産の特定

ISMSによれば，資産とは“組織にとって価値を持つもの”である。例えば，業務に使用する情報システムや媒体，建物・施設が資産である。

守るべき資産を特定するためには，まず守る範囲を定義して，その中から資産を見つける。守る範囲は，ISMSでは，“事業・組織・所在地・資産・技術の見地”から決めることになっている(**表1**)。

適用範囲を定義するのは，脅威が狙う対策の不備を見つけるためである。したがって，定義には，不備を見つけるために必要な情報を記載し，不要な情報を省く。例えば，想定した脅威が窃盗ならば，犯人の侵入経路が見つけやすいように，壁の有無や入り口の場所を平面図に定義するが，スプリンクラーの位置は不要である。コンピュータウイルスを使ったサイバー攻撃を想定するならば，IPパケットの流れを掴(つか)むためネットワーク層の構成を定義するが，通信ケーブルの配線に関する情報は不要である。

3.3 脅威が狙う脆弱性の特定

地震のような自然災害に対する脆弱性を特定するためには，被害が起きる原因を調べる。一方，コンピュータウイルスが狙う脆弱性を特定するためには，その目的と手口を調べる。ここでは，脅威の手口を分析する方法として攻撃ツリー(Attack Tree)[5]について述べる。

例えば，機密情報の取得を目的としてコンピュータウイルスを情報システムに送り込んでくる脅威については，**図1**のような攻撃ツリーを書く。

脅威の目的を一番上の箱に書き，手口を攻撃手順に分解して，順に下につなぐ。箱をつなぐ線には，andとorの2種類がある。andは，順に行う手順を示す。**図1**では，脅威の目的は，“機密情報を取得する”ことで，そのためには，“ウイルスをパソコンで実行”させ，“ウイルスがファイルサーバにアクセス”し，“ウイルスがデータを外部に発信”する。“ウイルスをパソコンで実行させる”ためには，“ウイルスをメールで届ける”か，“Webサイトからダウンロードさせる”。この二つの箱をつなぐ線にはandがないが，

表1．適用範囲の定義方法の例

項目	具体例	定義方法
事業	製品やサービス，それを提供する業務の流れ	業務フロー図，製品の仕様書
組織	業務を行う部署	組織図，正社員・非正社員の構成表
所在地	業務を行う場所	建物の住所，ハザードマップ
資産	建物・設備	建物の配置図，フロアの平面図
技術	情報システムの構成	ネットワーク構成図，ハード・ソフトウェア構成図

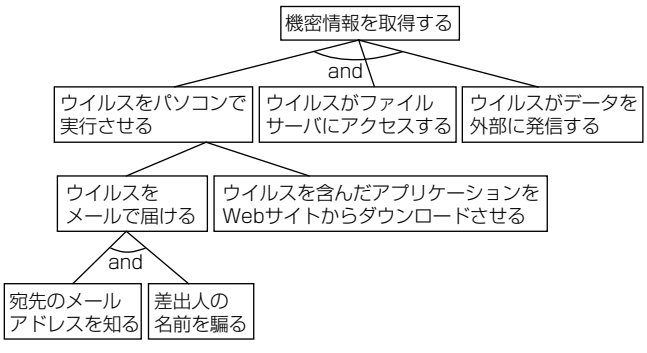


図1．攻撃ツリーの例

これはorを意味する。最後に，“ウイルスをメールで届ける”ために，“宛先のメールアドレスを知って”，“差出人の名前を騙(かた)る”。機密情報を取得するためには，一番下の左側の手順から順に実行すればよい。

脅威から機密情報を守るためには，各々の攻撃手順が狙う脆弱性をなくすことが必要である。**図1**の攻撃手順から脆弱性を求めた結果を**表2**に示す。

3.4 脆弱性対策の選定

ISMSは，脆弱性への対策を“管理策”と呼び，11のカテゴリーに分けて，133種類の選択肢を規定している(**表3**)。

各カテゴリーの最初の英字“A”は，選択肢がISMSの“附属書A”に記載されていることを示し，数字は，附属書Aでの通し番号である。これが5から始まるのは，管理策のガイドライン[6]とのつながりを示すためである。

脆弱性への対策として管理策を選択肢から選んだ例が**表4**である。説明として管理策の内容も追加した。

一つの脆弱性への管理策が二つ以上考えられる場合，管理策のガイドラインの記述が最も近い管理策を複数個選ぶことになっている。**表4**では，ウイルス対策の管理策として，“A.10.4.1 悪意のあるコードに対する管理策”と“A.10.4.2 モバイルコードに対する管理策”を選んだ。昨今のコンピュータウイルスは，JavaScript(注1)などのモバイルコードもあるからである。

最適な管理策が選択肢にない場合には，管理策を定義してもよい。**表4**では，サーバの機能を限定する“CM-7機能の限定”を，米国のガイドライン[7]から引用して追加した。

(注1) JavaScriptは，Oracle Corp. の登録商標である。

表2．攻撃手順で狙われる脆弱性の例

攻撃手順	脆弱性
宛先のメールアドレスを知る	従業員の氏名からメールアドレスが類推できる
差出人の名前を騙る	メールの差出人を本人確認できない
ウイルスをメールで届ける	パソコンにメールが届く
ウイルスを含んだアプリケーションをWebサイトからダウンロードさせる	外部のWebサーバからソフトウェアをダウンロードできる
ウイルスをパソコンで実行させる	ウイルスを実行する環境がパソコンにある
ウイルスがファイルサーバにアクセスする	パソコンからファイルサーバにネットワークでアクセスできる
ウイルスがデータを外部に発信する	パソコン又はファイルサーバから外部にデータが送信できる

表3．管理策のカテゴリー

カテゴリー	主な管理策の内容	管理策数
A.5 セキュリティ基本方針	基本方針の策定とレビュー	2
A.6 情報セキュリティのための組織	組織内の管理体制，外部組織と関係	11
A.7 資産の管理	資産の分類，ラベル付け，台帳管理	5
A.8 人的資源のセキュリティ	正社員・非正社員など要員の管理	9
A.9 物理的及び環境的セキュリティ	建物や設備の設置や運用	13
A.10 通信及び運用管理	情報・通信システムの運用，その稼働状況の監視	32
A.11 アクセス制御	アクセス制御方針の策定，情報システムの利用者の管理，ネットワークの構成	25
A.12 情報システムの取得，開発及び保守	情報システムの開発・調達の際のセキュリティ要件	16
A.13 情報セキュリティインシデントの管理	情報セキュリティ関する事件や事故の報告と対応	5
A.14 事業継続管理	事業継続計画の策定と実施	5
A.15 順守	個人情報保護法，不正アクセス禁止法等の法令の遵守	10

4. 管理策のプロセス統合

先に述べたようにして選んだ管理策は，実施する順序が決められた1つのプロセスとして統合し，情報セキュリティ対策の要件として定義する。これらのプロセスには2種類ある。一つは，多層防御(Defense-in-Depth)[8]であり，もう一つは，予防・発見・是正である(**表5**)。

多層防御とは，守る対象を中心にして，脅威が侵入してくる経路で遠くから近くへレベル分けし，レベルごとに防御ラインを敷くことをいう。

表5では，インターネットからネットワークを経由して悪意のある者がサーバを攻撃することを想定して，**図2**に示すように，レベルを三つに分けた。レベル1の防御ラインにはファイアウォールを設置し，ネットワーク利用方針を決めて，インターネットと内部ネットワークとの通信を制限する。レベル2の防御ラインは，ネットワークをつなぐファイアウォールとパソコン上のウイルス検知ソフトウェアである。レベル3の防御ラインは，サーバ自身であり，脆弱性を減らすために，クライアントに提供するサービス

表4．選んだ管理策の例

脆弱性	管理策(内容)
従業員の氏名からメールアドレスが類推できる	A.11.5.2 利用者の識別及び認証 (メールアドレスの形式を変更)
メールの差出人を本人確認できない	A.12.3.1 暗号による管理策の利用方針 (メールに電子署名)
パソコンにメールが届く	※対策しない：メールをパソコンで受信する必要が業務上あるから
外部のWebサーバからソフトウェアをダウンロードできる	A.11.4.1 ネットワークサービスの利用についての方針(ソフトウェアのダウンロードを禁止)
ウイルスを実行する環境がパソコンにある	A.10.4.1 悪意のあるコードに対する管理策 (添付ファイルなどを点検) A.10.4.2 モバイルコードに対する管理策 (実行を一部，禁止)
パソコンからファイルサーバにネットワークでアクセスできる	A.11.4.5 ネットワークの領域分割 (サーバを別のネットワークに設置) CM-7機能の限定 (クライアントに提供するサービスを限定)
パソコン又はファイルサーバから外部にデータが送信できる	A.10.6.1 ネットワーク管理策 (ファイアウォールで送信を制限)

表5．管理策をつないだプロセス

	レベル1	レベル2	レベル3
予防	A.10.6.1 ネットワーク管理策 A.11.4.1 ネットワークサービスの利用についての方針	A.10.4.1 悪意のあるコードに対する管理策 A.10.4.2 モバイルコードに対する管理策 A.10.6.1 ネットワーク管理策 A.11.4.5 ネットワークの領域分割 A.11.5.2 利用者の識別及び認証 A.12.3.1 暗号による管理策の利用方針	CM-7 機能の限定
発見	A.10.10.1 監査ログの取得 A.10.10.2 システム使用状況の監視 A.13.1.1 情報セキュリティ事象の報告		
是正	A.13.2.1 責任及び手順		
共通	A.8.2.2 情報セキュリティの意識向上，教育及び訓練		

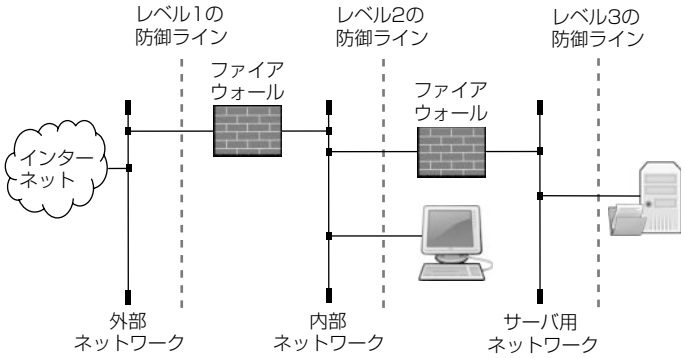


図2．ネットワークでの多層防御の例

やインストールする運用ソフトウェアを制限する。多層防御全体として，レベル1の防御ラインが突破されたらレベル2で，それが突破されたらレベル3で防御するように管理策を実行する。

予防・発見・是正は，管理策を実行するタイミングが，事件や事故が起きる前か，起きたときか，起きた後かで分けられる。予防では，事件や事故が起きるのを防ぐ。発見では，事件や事故が起きたことを発見する。是正では，事件・事故の拡大を防ぎ，情報システムなどを回復する。

筆者の経験では，攻撃ツリーに基づいた脆弱性への対策は，脅威が目的を達成するのを防ぐことを考えるあまり，予防に偏る傾向がある。そのため，**表5**には，発見と是正を追加した。発見には，不正なパケットを検知するため“A.10.10.1 監査ログの取得”，“A.10.10.2 システム使用状況の監視”，“A.13.1.1 情報セキュリティ事象の報告”を，是正には，事件や事故の対応体制と手順を整えるための“A.13.2.1 責任及び手順”を含めた。“責任及び手順”とは，情報セキュリティの事件や事故の管理における責任と手順の意味である。

さらに，管理策全体について“A.8.2.2 情報セキュリティの意識向上，教育及び訓練”を追加した。メールの電子署名，システムの監視，事件・事故の対応等の手順をシステム管理者と利用者に教育する必要があるためである。要員の教育は，無視又は軽視されることがあるが，管理策の実行には必要であり教育内容と実施時期を必ず計画すべきである。

リスクアセスメントでは，想定した脅威の手口に対応するように管理策を選択するので，プロセスでの管理策同士のつながりが見えにくいが，このような表を埋めていけば，足りない管理策を追加して，効果的で効率のよい情報セキュリティ対策の要件を導き出すことができる。

5. むすび

情報セキュリティ対策の要件を定義する手順をISMSでのリスクアセスメントと具体的な方法を交えて述べた。今後もISMS導入・維持のコンサルティングを通し，顧客の実情にあった情報セキュリティ対策の要件定義を提示していく。

参考文献

(1) JIS Q 27001：2006 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，一般財団法人日本規格協会（2006）
(2) JIS Q 9001：2008 品質マネジメントシステム―要求事項，一般財団法人日本規格協会（2008）
(3) JIS Q 14001：2004 環境マネジメントシステム―要求事項及び利用の手引，一般財団法人日本規格協会（2004）
(4) 金谷　治 訳注：新訂孫子，岩波文庫（2000）
(5) Schneier, B.：Secrets and Lies：Digital Security in a Networked World, Wiley（2000）
(6) JIS Q 27002：2006 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の実践のための規範，一般財団法人日本規格協会（2006）
(7) NIST Special Publication 800-53 Revision 3 Recommended Security Controls for Federal Information Systems and Organizations，NIST（2009）
(8) Homeland Security：Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies，US-CERT（2009）