

第一回：マインドマップで学ぶ、技術者のためのシステムセキュリティ対策入門

梅原 伸行¹

この連載は、IT業界でもにわかには脚光を浴びている「マインドマップ」という図表技法を使って、技術者の方向けにセキュリティ対策周辺を図解していこうというものです。

「マインドマップ」では、中心にテーマを据えて、放射状にトピックを（通常時計回りに）並べていき、さらに個々のトピックを掘り下げたサブトピックを枝状に広げていくという、いたってシンプル

しての活用が注目されています³。IT業界では、ブレインストーミングの際に使ったり、要求仕様をまとめたり、議事録を取るためのツールとしても利用され始めているようです⁴。

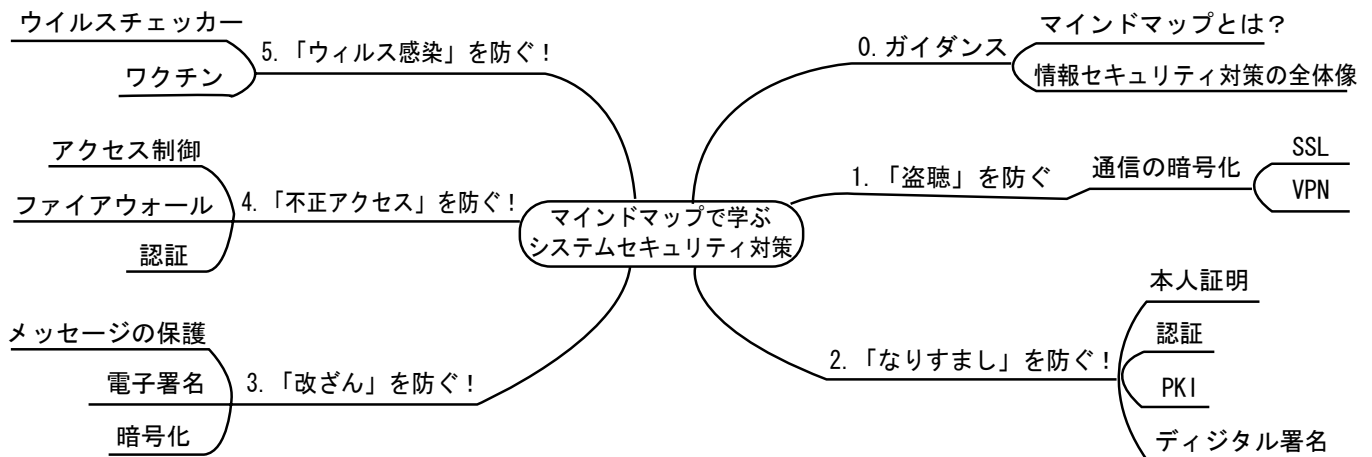


図1 本連載のアジェンダ

まず始めに、「マインドマップ」²について簡単に説明をしておきたいと思います。「マインドマップ」云々については、ちまたの書籍に譲りますが、例えば、本連載のアジェンダを「マインドマップ」で書くと、図1のようになります。

な記述ルールとなっています。イラストやマークなどを入れてカラフルにするとより美しく楽しいマップができます。

この「マインドマップ」のどこが良いのかというと、一般に「直感的で分かりやすい」とか「記憶しやすい」などと言われていますが、「コミュニケーションツール」と

「マインドマップ」は、メモ用紙やホワイトボードに思いついたままに書き込むというのが「基本」ですが、やはり、人に見せるにはきれいにフォーマットしたいというのが自然な欲求であり、ちゃんとその欲求を満たすツールが幾つかあります⁵。本稿では「JUDE Professional」⁶という国産 CASE

1. JIPDEC ISMS 審査員補、SAAJ システム監査人補
 2. お勧めは発案者による「ザ・マインドマップ」トニー・ブザン(著)ダイヤモンド社
 3. 似たようなものに「偏愛マップ」というものもあります。「偏愛マップーキラいな人がいなくなるコミュニケーション・メソッド」齋藤孝(著)NTT出版
 4. 筆者は、1994年頃からマインドマップを開発の現場で要求仕様の整理などのために利用していましたが、当時は今ほど知られておらず、「何だ、この変な図は」と一蹴されたものです。今も十分周知されているとは言えませんが。
 5. "MindManager", "FreeMind" など。Visio のテンプレートにも似たようなものがありますが、使い勝手が直感的ではありません。"FreeMind" も私的には操作感がいいでした。
 6. 開発元は永和システムマネジメント。「JUDE」は「UMLお絵かきツール」としてとても使い勝手が良いです。また、マインドマップからユースケースに変換する機能もあります。なお、「JUDE Communication」というフリー版もありますが、そちらでは「マインドマップ図」は「見るだけ」なので要注意。他に、印刷時に「JUDE」ロゴが表示されるなど、機能制限あり。

ツール⁷の「マインドマップ図」を使っております。

さて、本連載のメインテーマである「セキュリティ対策」の話に入りますが、「情報セキュリティ対策の全体像」を早速マインドマップでまとめてみると図2のようになります。

「個人情報漏洩」に代表されるような情報セキュリティ事件・事故の危険を軽減するための対策を「情報セキュリティ対策」と言いますが、一般に図に挙げられている「物理的・環境的セキュリティ対策」・「システムセキュリティ対策」・「人的・管理的セキュリティ対策」から成ります。

さて、セキュリティ事件・事故の原因の大半⁸が、従業員の「不注意」や「持ち出し」、「盗難」な

ど「人的要因」であると言われていますが、この現状を踏まえると、セキュリティ対策として最も有効なのは「人的セキュリティ」ということとなります。これには、社員のセキュリティ意識を高める教育や会社のセキュリティ方針（情報セキュリティポリシー）を周知徹底すること、内部監査の実施などが含まれています。

しかし、この「人的セキュリティ」は、基本的に「忘れない」、「気をつける」といった約束を守ることによって成り立っているため、社員の間で意識にばらつきが生じたり、過失による事故発生の可能性もないとは言えません。また、手順を複雑にすれば、その分、業務効率が低下する可能性もあります。

そこで、業務効率を一定の水準

に保ちつつ「人的セキュリティ」の負担を軽減するために、「システムセキュリティ対策」を上手に組み合わせます⁹。

「システムセキュリティ対策」は、情報システムそのものに事件・事故から経営資源を保護するための仕組みを設けるもので、具体的には通信の暗号化や認証、デジタル署名、アクセス制御などがあります。

本連載では、情報セキュリティ対策の全体像のうち、この「システムセキュリティ対策」にフォーカスをあて、「情報資産」¹⁰の「脅威」¹¹となっている「盗聴」・「なりすまし」・「改ざん」・「不正アクセス」・「ウイルス感染」に対するセキュリティ対策のポイントを解説していききたいと思います。

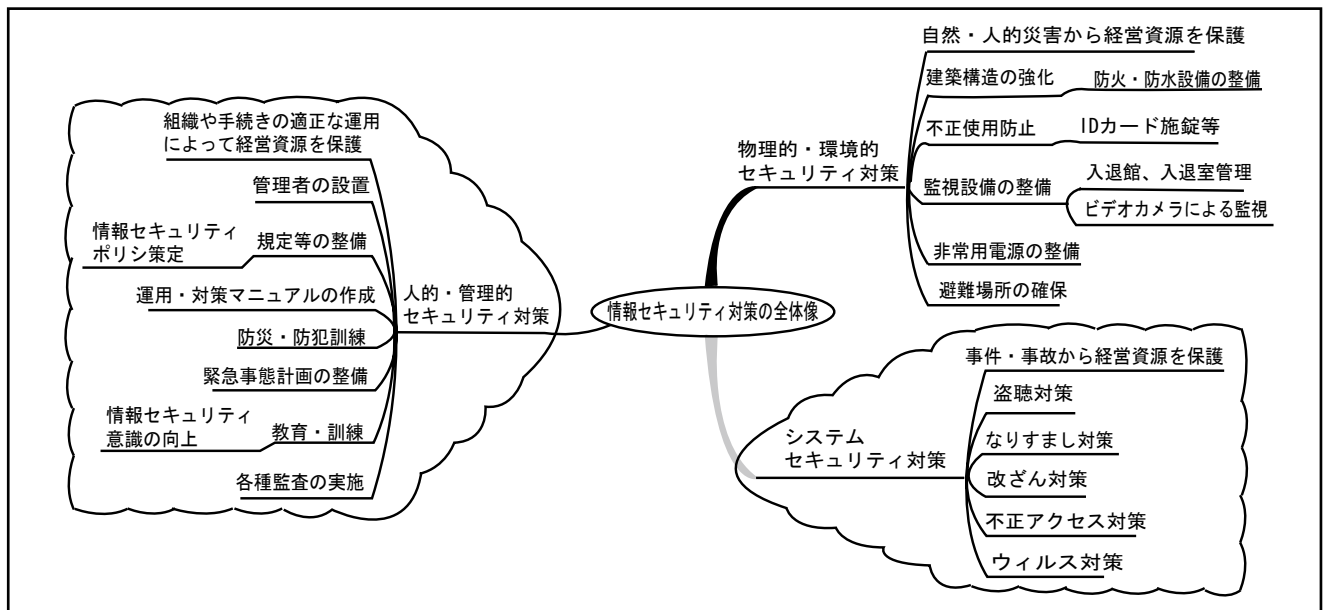


図2 情報セキュリティ対策の全体像

7. 筆者はかつて「Rational Rose」という米国製 CASE ツールを愛でておりましたが、大変高価である割によく落ちたものです。「JUDE」は長時間使っても不安定にならないというのがとても心地良いです。(当たり前なのですが)

8. 2005/3 国民生活センターの調べによると 68%。ちなみに、「システム上の問題」は 12%。

9. 最初に「システムセキュリティ対策」ではなく、「人的セキュリティ対策」

を考えるのが MECE 的 (もれなく重複なし) セキュリティ対策のポイントです。

10. 情報セキュリティでは、情報を保存し保管・活用するための「情報システム」だけでなく、組織が所有しビジネスで活用するすべての情報を含めた「情報資産」を安全に守るという考え方をします。

11. 脅威：情報資産に影響を与え損失を発生させる直接の原因。事故の潜在的原因。