監修者が語る！
なぜ基礎が大事なのか、知っていてほしい「セキュリティの土台」とは

暮石 和宏
シスコシステムズ合同会社
エンタープライズソリューションズエンジニアリング本部
ソリューションズアーキテクト

2026年1月15日

2025年ニュースの見出しから振り返る 様々なサイバー攻撃と被害

ランサムウェア・業務停止関連

- ✓ ○○社、ランサムウェア被害で受注、出荷停止
- ✓ サイバー攻撃でシステム障害、復旧メド立たず
- ✓ 身代金要求型ウイルス、国内製造業を標的
- ✓ 基幹システムダウン、決算発表を延期
- ✓ 「データを暗号化した」犯行グループが犯行声明

個人情報・機密情報の流出

- ✓ 顧客情報○○万件流出かサーバーに不正アクセス
- ✓ クレジットカード情報漏洩の可能性、ECサイト一時閉鎖
- ✓ マイナンバー含む個人データ、委託先から流出
- ✓ ダークウェブ等で機密情報や個人情報、顧客リスト等が暴露される
- ✓ 社内メール丸見え、フィッシング詐欺でID奪取

サプライチェーン・関連企業の被害

- ✓ サプライチェーン攻撃、取引先経由で本社へ侵入
- ✓ 「踏み台」にされる中小企業、セキュリティ対策急務
- ✓ 海外子会社でウイルス感染、国内ネットワークへ波及
- ✓ 約○社に1社がサイバー被害を経験（最新調査）
- ✓ 関連会社への攻撃で自動車生産ラインが停止

国家・インフラ・新技術関連

- ✓ 重要インフラ狙うサイバー攻撃、政府が警戒感
- ✓ 防衛産業へハッカー集団攻撃、機密情報狙う
- ✓ 病院システムにサイバー攻撃、電子カルテ閲覧不能に
- ✓ AI悪用の巧妙な手口、偽メール見破れず
- ✓ サポート終了のOSに穴、脆弱性突くゼロデイ攻撃

情報を適切に取捨選択しながら、背景も含めて正しく状況を理解した上で、
各自が適切な対応を行う為には、情報セキュリティに関する基礎的知識が必要となる⇒
立場(学生、社会人、経営者等)の違いによらず、継続的に学ぶことが必要

※情報セキュリティに関する基礎的知識(以後、基礎知識とする)

立場の違いと異なる視点/分析/対応

教員

基礎知識
+ 専門分野の知識
+ 教育者としての視点/分析/対応

社会人(IT管理者)

基礎知識
+ IT技術者としての知識
+ 業務関連の知識
+ IT技術者としての視点/分析/対応

経営者

基礎知識
+ 業務関連の知識
+ 経営関連の知識
+ 経営者としての視点/分析/対応

A社サイバー攻撃による被害 出荷停止

ネットワーク機器や端末などの複数経路から侵入の疑い

仮に自分や自社が関係していたならばどうか?

基礎知識
+ 情報処理関連の知識
+ 学生として視点/分析/対応

学生

基礎知識
+ 業務関連の知識
+ ITを活用する社会人としての視点/分析/対応

社会人(ITのユーザ)

基礎知識
+ IT技術者としての知識
+ 業務関連の知識
+ 関連するテクノロジーに関する知識
+ IT関連の開発者としての視点/分析/対応

社会人(IT関連の開発者)

立場の違いと異なる視点/分析/対応 + 気づきの共有

教員

基礎知識
+ 専門分野の知識
+ 教育者としての視点/分析/対応

社会人(IT管理者)

基礎知識
+ IT技術者としての知識
+ 業務関連の知識
+ IT技術者としての視点/分析/対応

経営者

基礎知識
+ 業務関連の知識
+ 経営関連の知識
+ 経営者としての視点/分析/対応

気づきの共有には
「土台としての基礎知識
+ 心理的安全性」
が不可欠

A社サイバー攻撃による被害 出荷停止

ネットワーク機器や端末などの複数経路から侵入の疑い

仮に自分や自社が関係していたならばどうか?

基礎知識
+ 情報処理関連の知識
+ 学生として視点/分析/対応

学生

基礎知識
+ 業務関連の知識
+ ITを活用する社会人としての視点/分析/対応

社会人(ITのユーザ)

基礎知識
+ IT技術者としての知識
+ 業務関連の知識
+ 関連するテクノロジーに関する知識
+ IT関連の開発者としての視点/分析/対応

社会人(IT関連の開発者)

情報セキュリティに関する基礎的知識(基礎知識)とは(抜粋)

情報セキュリティとは

守るべきもの(= 情報資産) を脅かすもの(= 脅威)から守るための技術や体制

情報セキュリティにおける脅威は、3つに分類される

人的脅威: 「人」の行動やミス、悪意によって引き起こされる脅威

技術的脅威: コンピュータやネットワークの仕組みを利用した攻撃、またはシステムの不具合による脅威

物理的脅威: 物理的な手段や自然現象によって、情報資産やシステムが損なわれる脅威

リスクと脅威の違い

脅威 (Threat) = 「危害を加える要因(原因)」

リスク (Risk) = 「実際に脅威が発生し、それによって損害や損失が発生する可能性(結果)」

情報セキュリティに関する基礎的知識(基礎知識)とは(抜粋)

脆弱性とは

情報資産やシステム、組織における「弱点」や「欠陥」(一般的には、セキュリティホールとも呼ばれる)

例: ソフトウェア・ハードウェアの欠陥(バグ)、設定の不備(設定ミス)、人や運用の弱点(プロセス・人間)

脅威(攻撃者) はコントロールできませんが、脆弱性(弱点) は、ソフトウェアのアップデート(パッチ適用)や設定の見直しによって、自分たちで塞ぐことが可能

⇒ セキュリティ対策の基本は「脆弱性をいち早く見つけ、塞ぐこと」

情報セキュリティの3要素(CIA)

機密性 (Confidentiality): 許可された人だけが、情報にアクセスできること

完全性 (Integrity): 情報が正確で、改ざんされていないこと

可用性 (Availability): 必要な時にいつでも、情報やシステムが使えること

例: 情報セキュリティに関する基礎的知識(基礎知識)習得の流れ

1. 基礎概念と管理

「何を守るか」「どう管理するか」の土台作り

基本原則: CIAの3要素（機密性・完全性・可用性）、脅威（人的・技術的・物理的）、脆弱性の定義

管理とリスク: ポリシー策定、ISMS、リスクアセスメント、法的要件の理解

目的: 技術論の前に、組織としての守るべき指針とルールを確立する

2. 技術的基盤

攻撃と防御の舞台となる「ネットワーク」の理解

ネットワーク: TCP/IP、プロトコル、DNS、Webシステムの構造

目的: 攻撃者が通る「道」と、守るべき「場所」の仕組みを把握する

3. 脅威と防御技術

「敵の手口」を知り、「守る技術」を学ぶ

攻撃手法: マルウェア、DoS攻撃、標的型攻撃、AI脅威、脆弱性攻撃

ネットワーク防御: 暗号化、認証・認可、PKI、通信制御

エンドポイント防御: OSセキュリティ、デバイス管理、物理対策

目的: 具体的な攻撃手法に対し、多層的な防御策（NW・端末）を適用する

4. 運用と対応

インシデント発生時の「実務対応力」

インシデント対応: 検知、分析、ログ調査、コマンド操作

脆弱性管理: 継続的な弱点の修正とアップデート

目的: 攻撃を受けた際に被害を最小限に抑え、復旧させる能力を養う

CCSTサイバーセキュリティの本を出すに至った経緯

- シスコジャパンの中期成長戦略の3つの柱の一つとして1つとして「持続可能な未来の創造」
  - ✓「持続可能な未来の創造」の1つとして「デジタル人材育成」

- 昨今(2024年初頭)どのような人材が求められているのだろうか
  - ✓ セキュリティ関連の人材が少なく、不足している
  - ✓ **セキュリティの専門家だけではなく、デジタル社会では一般的な利用者においても、基礎的なセキュリティのリテラシーを身に着けていないと脅威に対応できない**

- セキュリティの基礎知識を持つ人材の裾野を広げるためには何ができるか
  - ✓ ネットワーキングアカデミーで無償のオンライントレーニングを提供する
  - ✓ CCSTサイバーセキュリティ試験(日本語/英語等)
  - ✓ 日本語で受験できるのに、日本語で学べる本がなかった…
    ~~しかも、英語版の本を見てみても分厚くてそれなりに難しい~~ ⇒ なら書くか/書いてもらうか

監修者としての想い

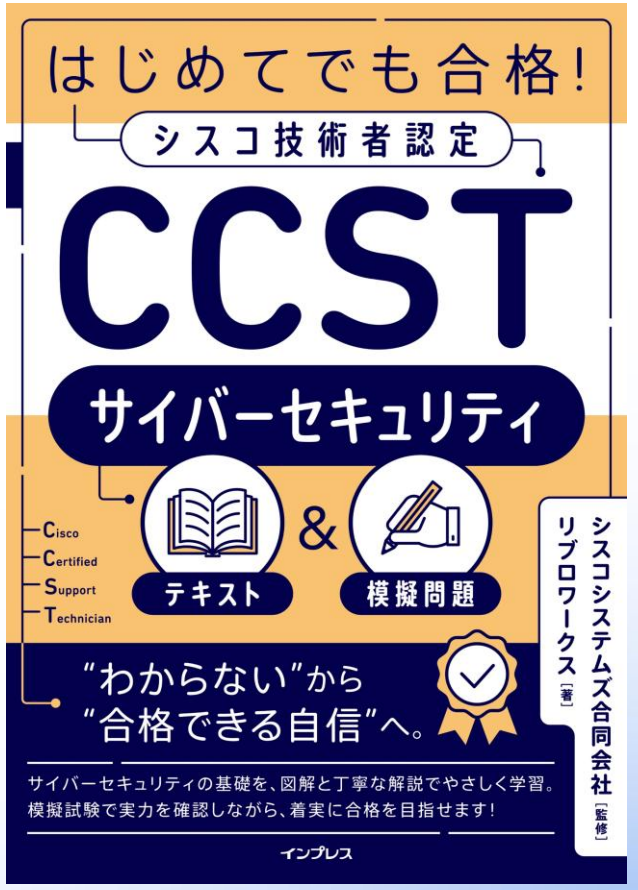
- CCSTサイバーセキュリティ向けの学習本ではあるが、単に資格の対策のみにフォーカスした内容にはしたくなかった

- デジタル社会で一般の利用者(学生や社会人)にも求められるセキュリティ関連のリテラシー(基礎的な知識)についても学べるものにしたい

- CCSTサイバーセキュリティを取得後に、ITパスポート等を受験しても役立つ基礎的な内容や考え方も可能な限り網羅的に入れることを意識して構成
※逆に、ITパスポートを受験した方々が読んでも理解し易いのではないか

- 色々書いてもらいたい/書きたいのをぐっと抑えながら、必ず知って欲しい内容については咀嚼しながら丁寧に説明する/監修者として全体構成・修正・加筆を行う

ご参考: CCSTサイバーセキュリティ本の構成



目次:

(A5判、二色刷り、全232ページ)

公式サイト
https://book.impress.co.jp/books/1124101144

最後に

立場によらず、各自が適切な対応を行い、互いに気づき等を共有する為には
土台となる「サイバーセキュリティに関する基礎的知識」が必要であり、
変化に合わせて継続的に学び続けることが重要

学生/教員の皆様へ

テクノロジーは常に進化しており、我々に様々なメリット/デメリットをもたらします。
しかし、攻撃者にとっても同様で、常に新しいテクノロジーの活用法を考えます。
「常に学び続ける好奇心」が最強の武器です。

社会人の皆様へ

セキュリティはIT部門だけの仕事ではありません。
ITのユーザとしても「自分ごと」として捉え、怪しいメール等を開かないなどの基本動作を徹底しましょう。

経営者の皆様へ

セキュリティ対策は「コスト」ではなく、ビジネスを継続するための「リスク管理」です。
事故が起きた時の損害や信用の失墜は、対策費用を遥かに上回る傾向があります。


CISCO