**セキュリティ仕様策定プロセス（案）**

～Windows Active Directory環境用セキュリティガイドライン対応～

2020年3月

セキュリティ検討プロジェクトチーム

**《目次》**

１　序章　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　2

2　セキュリティ仕様策定の課題とセキュリティガイドライン　 ・・・・・・・・・・・・・・・・　8

３　セキュリティ仕様検討プロセス　・・・・・・・・・・・・・・・・・・・・・・・・・・・・　13

【参考1：セキュリティ策定の現状と課題】　・・・・・・・・・・・・・・・・・・・・・・・・　23

【参考2：SQLインジェクション事件（東京地裁平成26年1月23日判決）】　・・・・・・・・　27

【参考3：セキュリティ仕様策定プロセスイメージ図】　・・・・・・・・・・・・・・・・・・・　29

【参考4：緩和策実装検討シート例】　・・・・・・・・・・・・・・・・・・・・・・・・・・・　30

【参考5：デフォルト緩和策　端末編　＜一覧表＞】　・・・・・・・・・・・・・・・・・・・・　31

【参考5：デフォルト緩和策　端末編　＜詳細＞】　・・・・・・・・・・・・・・・・・・・・・　32

【参考6：デフォルト緩和策　セキュリティ仕様・Webアプリケーション編】 ・・・・・・・・・　42

【参考7：汚染される開発環境】　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・　46

【参考8：セキュアコーディングガイド】　・・・・・・・・・・・・・・・・・・・・・・・・・　47

## 序章

### 背景

情報技術（IT）の活用が、広く社会に影響を及ぼす時代になっている昨今において、パソコンやスマートフォン、メールやWebなどの利用は勿論のこと、事業におけるサービスや内部の業務においてもITは活用されている。またIoT（Internet of Things）化やAI（Artificial Intelligence）の活用が進むことで利便性が向上し、多数の機器から得られたデータは、組織の新たなサービス提供や品質向上など、広くは組織の経営に活かされている。個人や組織における活用や技術革新が進めば進むほど、サイバー空間における攻撃も増加、巧妙化し、個人や組織が持つ端末やデータなどは継続的に狙われている。**【参考1：セキュリティ策定の現状と課題】**

こうした本格的なIT活用が進む中、ウェブアプリケーションの開発委託契約において、ユーザーとベンダーがセキュリティ仕様を合意することなく開発を行い、結果としてサイバー攻撃を受けてクレジットカード情報等が漏洩した事案において、ベンダーが債務不履行に基づく損害賠償義務を負うとする下級審判決が出されるなど、セキュリティ対策をめぐってベンダーの責任が問われるケースが複数生じている。 **【参考2：SQLインジェクション事件】**

さらに、2020年4月から施行される改正民法では、請負契約における契約不適合に関する担保責任の規律が一新された。これに伴い、ベンダーは、開発当時のセキュリティ水準に沿ったセキュリティ対策を納入物に施していなければ、長期にわたる担保責任を負う場合も考えられる。改正民法のもとでは、ソフトウェアに存在する脆弱性が契約不適合に該当するような場合や、ベンダーの重大な過失により脆弱性があることを知らずにユーザーに引き渡した場合には、担保責任の期間制限が適用されないことなどにも留意が必要である。一方でユーザーはセキュリティ要件に必要な情報の提供とセキュリティ対策の実装ポリシーの判断において一定の責任を負うことが求められる状況となった。

このような状況を鑑み、情報システム開発委託契約に基づく開発プロセスにおいて、最新の脅威情報を反映したリスクベースでのセキュリティ対策を、より具体的な表現で実装方法が参照できる新しいガイドラインが必要であり、ユーザーが情報システムを調達する場面において、このようなガイドラインを参考にして最適なセキュリティ仕様策定を完成させるには、如何にユーザーとベンダーがシステム開発業務プロセスにおいて互いに協力し責任を果たすか、ということが重要となる。

### 目的

このセキュリティ仕様策定プロセス（以下、モデルプロセス）は、前述の新しいガイドラインである「セキュリティガイドライン（Windows環境編）」（以下、セキュリティガイドライン）を参考にすることを前提に、情報システム調達に伴うシステム開発業務プロセスにおいて、最適なセキュリティ仕様を策定する為の理想的なモデルプロセスとして解説したもので、ユーザーおよびベンダー相互がなすべき詳細プロセスと、それに関連する管理業務について紹介している。その例として本章のプロセス毎の解説では、開発業務の最初のプロセスである「企画支援」の段階から、ユーザーはセキュリティガイドラインを参考にシステムの調達を目的とした実施計画を得られるようベンダー候補者に対し、RFIを通してセキュリティガイドライン対応の可否に関する情報収集を実施することを求めている。

### 本章の構成と使い方

セキュリティガイドラインは、ユーザーとベンダーの双方が情報システムの開発における共通の課題とそれに見合った適切なセキュリティ要件を合意するために利用されることを目的とした引用ドキュメントであるのに対し、本モデルプロセスは、セキュリティガイドラインを参考に、各プロセスにおいて＜ユーザー側＞、＜ベンダー側＞、＜ユーザーとベンダー間の協議＞からなるセクションで解説し、個々のプロセスを適切に実施するための関連業務や管理策について紹介する。

**※[成果物]はセキュリティ関連文書に限る**

**企画支援：**

このプロセスは、**(1) システム化構想**、**(2) システム化計画**、**(3)提案**、からなり、ユーザーのシステム調達目的と計画を把握した上で、セキュリティガイドラインを参考に具体的なセキュリティ対策実装が可能なベンダーを選定するための提案書を得ることを目的とするプロセス[[1]](#footnote-1)。

[成果物] RFI、RFP(外部設計作成時の場合もあり)、提案書

**要件定義作成支援：**

このプロセスは、**(4) 要件定義**、であり、要件定義書の作成に必要となるユーザーの情報提示とベンダーの要件定義作成支援に関するプロセス。

[成果物] 要件定義書

**外部設計作成（支援）：**

このプロセスは、**(5) システム要件定義**、であり、ソフトウェア開発業務を開始する前までにセキュリティ仕様を確定させ、外部設計書およびセキュリティ仕様書を策定するプロセス。

一部のユーザーでは、業務システムの調達・拡張・刷新において独自のセキュリティ仕様を実装する必要があり、ユーザーによる外部設計からの要件をRFPに反映し、それを実装可能とするベンダーを選定するプロセスでもある。

[成果物] 外部設計書、セキュリティ仕様書初版、（RFP）

**ソフトウェア開発業務：**

このプロセスは、**(6) ソフトウェア詳細設計**、**(7) ソフトウェア構築**、**(8) システム結合**、からなり、外部設計書およびセキュリティ仕様書に基づいてソフトウェア開発を実施するプロセス。

[成果物] 内部設計書、プログラム、システム結合テスト結果報告書

**ソフトウェア運用準備移行支援業務：**

このプロセスは、**(9) システムテスト**、**(10) 導入・受入支援**、**(11) 運用テスト**、からなり、各システム要件に基づく実装の適合性、実環境への導入と納入準備の確認、当初のシステム調達目的の確認を実施するプロセス。

[成果物] セキュリティ仕様書最終版

**運用業務：**

このプロセスは、**(12) 運用**、であり、意図された環境で納入されたシステムを運用し、ステークホルダーへのサービスを提供するプロセス。SLAに基づき、サービスレベル維持に必要な運用・保守に関連する契約を締結する。また、セキュリティ監視やCSIRT /PSIRTとの連携がある場合は、インシデント発生時の対応体制や役割に関する文書を更新する。

[成果物] 運用代行契約書、保守契約書、保守開発契約書など

モデルプロセスにおける、ユーザー・ベンダーの関連業務や管理策を連携づけたイメージ図を以下に示す。

**【参考3：セキュリティ仕様検討プロセスのイメージ】で拡大版を掲載A close up of a map

Description automatically generated**

図 ：セキュリティ仕様検討プロセスのイメージ

各プロセスに対し、ユーザーの責任において準備されるべき機能や仕組みと情報があり、同時にベンダーにも開発ベンダーの責任として管理されるべき標準やスキル管理などが必要となる。これらの双方の責務として相互の整合性を維持する努力が理想的なシステム開発委託契約履行につながると考える。

### ユーザー・ベンダー相互の責任

#### 相互補完的な情報の開示と記録

セキュリティ事故の原因となるインシデントを完全に無くすことは不可能である。これを前提としつつ、インシデントの影響を最小化するため、ユーザーとベンダーは当該ソフトウェアの開発の過程で各々どのような役割を担うこととするかを以下に示す。

1. ユーザーはシステムオーナーとして守るべき情報資産を明確にし、ベンダーに適時に伝え（変更が生じれば変更の内容も含む）、それらを常に維持する。
2. ベンダーは専門家として、限られたリソースを如何に効率よくインシデント発生の低減に費やすかを検討し、ユーザーに適時に留意事項・改善案等を明示する。

(a)の努力は(b)の実現の選択肢を増やし、(b)は(a)を実現する可能性を高めるという点で、ユーザーとベンダーの役割は相互補完的であるといえる。

ユーザーに引き渡される当該ソフトウェアは、インシデント発生を低減する工夫と努力の成果でなければならないが、これらの検討の記録は、要件定義から開発に至る各プロセスにおいて作成されるシステム仕様書等のドキュメントや議事録において、検討事項とその結果（リスク受容を含む）を見える化、明示化しエビデンスとして残すことが必要である。

#### セキュリティ仕様の確定時期

ユーザーはシステムオーナーとしてセキュリティ仕様を確定する義務を持ち、セキュリティバイデザインの発想で開発着手前に仕様が確定していることが理想となる。開発工程が進んでしまってからセキュリティ対策を講じるには限界があり、セキュリティ投資が過大となるおそれが高い。一方、外部設計工程が終わらないとセキュリティ仕様を確定させることは困難であるため、セキュリティ仕様の確定はソフトウェア開発業務プロセス（後述）を開始する前までに完了することが重要となる。

#### セキュリティ仕様確定の主体

セキュリティ仕様の内容確認は、ユーザー自身の事業計画、予算（リソース）、及びリスクマネージメントとの整合性が担保されていることが前提となる。これらの要素がセキュリティ仕様の中身を大きく左右することから、ユーザーはその責任においてセキュリティ仕様を適時適切に確定させる役割を担うとするのが合理的である。

#### セキュリティ仕様策定に際してのベンダーの役割

ベンダーはソフトウェア開発の専門的知見と経験を有することから、ユーザーが当該ソフトウェア開発で目標とする業務効率化や付加価値向上を理解し、同時にその実現に必要となるセキュリティ要件の具備について、ユーザーと協力することが必要である。

故に、ベンダーはユーザーがセキュリティ要件を検討するために必要な情報や専門知識・ノウハウ等を必要に応じて提供し、ユーザー自身が適時適切にセキュリティ仕様を確定できるように適切な留意事項・改善案等を明示することが求められる。

#### セキュリティ仕様に盛り込むべき事項

セキュリティ仕様については、当該ソフトウェアの作成目的、当該ソフトウェアの使用環境、OS、言語等により一律に決めることは難しいが、セキュリティガイドライン以外に、最低限実施すべき設定等を設けた。これについては後述（3.3 外部設計作成プロセス/ (5)システム要件定義/ デフォルト緩和策、及び【参考5：デフォルト緩和策】）を勘案しつつ、その納入の時点で政府が民間事業者に求めるセキュリティ水準を達成するものとすることが望ましい。なお、Windows及びLinuxで稼働するソフトウェアを想定した具体的なセキュリティ仕様としては、IPAが公表するセキュリティガイドラインを参照することができる。

#### 運用段階

当該ソフトウェアの要件定義から設計・開発に至る各段階でユーザーとベンダーが相互に協力し、サイバーセキュリティに十分に配慮された当該ソフトウェアの引渡しがなされたとしても、引渡しの翌日から、新たな脆弱性が発見され、当該ソフトウェアに新たな脅威が生じるなどの可能性を完全に払拭することはできない。

このため、ユーザーとベンダーは、必要に応じて稼働状況のモニタリングや個別のセキュリティ対応も含めたサポート契約の締結、ユーザーとベンダー又はセキュリティ専門事業者間の契約による定期的なセキュリティ診断の実施など、セキュリティリスクの顕在化に備えた予防的措置のあり方を協議・検討することが望ましい。

#### セキュリティインシデント発生時

ユーザーにおいて現実にセキュリティインシデントの被害が発生し、セキュリティ専門事業者等による緊急時対応が必要になった場合、ベンダーは、ユーザーの求めに応じて、ユーザーにおける問題の解決に資する情報の提供など一定の協力を行うことが望ましい。このためには、ベンダーは、ユーザーに引き渡した当該ソフトウェアの複製物や取引の記録等を保管することが必要となるため、保管対象、保管期限や保管方法等については、当該ソフトウェアの引渡し等に際して予め合意するか、ユーザー・ベンダー間のサポート契約等が締結されている場合には、その契約等において合意することが望まれる。

インシデントが発生した場合、ユーザーはステークホルダーに対し事実（何が起きたか）、考えられる影響範囲、対処方針を可能な限り早く正確に説明する責任がある。「調べる術がない」状況にならないためには、調査分析に必要な資産管理、構成管理、ログや運用記録、マネージメント・システムによる評価（課題と対策のエビデンス）などが重要となる。調査[[2]](#footnote-2)が進み、インシデントの原因がサイバー攻撃であった場合は、前述にある平時に記録したエビデンス（リスク受容理由を含め、セキュリティ仕様に関連するセキュリティ仕様検討事項とその結果を明示化したもの）が説明責任を果たすための基本情報[[3]](#footnote-3)となる。

## セキュリティ仕様策定の課題とセキュリティガイドライン

### セキュリティ仕様策定における課題

経済産業省のソフトウェア開発委託基本モデル契約書第1版（2007年）ではセキュリティを重視し、50条では、セキュリティ対策について、「その具体的な機能、遵守方法、管理体制及び費用負担等を協議の上書面により定めるものとする」と規定されている。もっとも、これまでには必ずしも十分なセキュリティ対策の協議がなされていたとはいえない事例も生じている。**【参考2：SQLインジェクション事件】**

また、講ずべきセキュリティ対策については、システム仕様書等に明示されるものの、一定のリスクを受容する判断により、関連するセキュリティ対策を講じることを見送った内容を記録にとどめる契約慣行が成立しているとは言い難い。対策を見送った事項についてインシデントが発生した場合、ベンダーの債務不履行、契約不適合責任などの存否を巡って紛議となることが考えられる。なお、セキュリティ仕様策定には、以下の課題が存在する。

#### ユーザーの課題

* 現行の情報システムを正確に把握していない
* 情報資産の棚卸が不完全で、重要情報が各所に偏在している
* リプレイスできない脆弱性を有するレガシー資産との連携

#### ベンダーの課題

* 年間で17,000件もの大量のソフトウェア脆弱性情報の存在[[4]](#footnote-4)
* 様々な攻撃手法の存在[[5]](#footnote-5)
* 専門性が高くかつ広範な知識が求められるため、ベンダー内の技術職でも情報量および技術レベルの格差が存在

#### ITコンポーネント供給者の課題

* 脆弱なデフォルト設定
* FOSSでのサポート停止

#### ユーザーの課題

多くのシステム開発契約でセキュリティ仕様の合意がなされていない原因として、ユーザー側には「ITベンダーを信頼している」、「そのための時間を買っている」、「複雑でよくわからない」、「サイバー攻撃とは無関係」といった考えが散見される。そのため、具体的な情報資産の防御が開発テーマに上がらず、その結果、サイバー攻撃の被害を受ける事案が多数存在する。ベンダーも、ユーザーから具体的な要求がなく、守るべき資産に対する判断が付きにくいため、要件定義、外部設計段階で具体的な仕様を盛り込めず、システム方式、プログラミング段階でセキュリティに配慮したコーディングが行われないのが現状である。そこで、モデル契約におけるセキュリティ仕様決定プロセスに、ユーザー環境で「何が充足されているか」、「何が不足しているか」をユーザーが自己認識できるプロセスを組み込むことを提案した。これによって、ベンダーへの丸投げが防止でき、不明点をベンダーに問い合わせるなどして、仕様の過不足や、セキュアコーディングの要求、機器の導入、設定の実施などを真摯に議論することが可能となる。

#### ベンダーの課題

脆弱性情報の更新数は多く、年間で17,000件もの大量のソフトウェア脆弱性情報が発信されており、攻撃者は脆弱性情報の発表直後にその脆弱性の有無を探索しており、SOC等ではそういったパケット受信量のピークが確認されることが常識となってきた。

ベンダーは専門性が高く広範な知識が求められ、脆弱性情報の更新頻度が高い状況においても担当する技術者のサービス品質が求められるため、ベンダー内部においてはSE標準や開発標準などでユーザーに対するサービス品質の底上げと標準化が求められると同時に正確でタイムリーな情報を社内基盤として整備することが望まれる。**※【参考3：セキュリティ仕様検討プロセスのイメージ】のベンダー側を参照**

#### ITコンポーネント供給者の課題

ベンダーおよびベンダーへのITコンポーネント供給者は、セキュリティを配慮した上で開発や提供を行う必要がある。Software ISACの調査によれば、ソフトウェア開発にあたって外部委託している割合は約８割、OSSの使用割合も7割を超えている。しかし、ソフトウェア脆弱性の取り扱いについて契約時には定めていなかったり、検証についても案件によって対応が異なったりする回答も見られた。供給者側も常にセキュリティを意識し、企画から廃棄までのセキュア開発ライフルサイクルの全てのフェーズにおいてセキュリティを考える必要がある。

### セキュリティ仕様確定手法の検討

JIS Q 27002 (ISO/IEC 27002）では、情報セキュリティは機密性、完全性、可用性を維持することと定義されている。このうち可用性におけるシステム停止は、単一障害点の除去や、冗長構成などのシステム構成で決定されるが、それ以外の機密性と完全性は、脆弱性管理とアクセス管理で概ねコントロールが可能と考えられ、これらを実現する管理の確からしさやコントロールが適切であるかの網羅的な把握、または検出といったモニタリングを実施することで維持が可能となると考えられる。

脆弱性管理は、ソフトウェア、機器のファームウェアに潜む脆弱性の排除であることから、対象のソフトウェアコンポーネントやファームウェアの所在とバージョン管理が重要となってくる。これに対して、アクセス管理は、情報資産の識別と識別された資産への読み取り、書き込み、変更、プログラムの場合は読み取りと実行の管理であり、そのための権限設定とネットワーク的なアクセス経路の管理設定といえる。

また、対策を目的としたこれらの管理は適切に実施されることではじめて対策として機能する。さらに、新たな攻撃手法や想定外の事象においても対処と分析を可能とするのがモニタリングといえる。

表 1：情報セキュリティの定義と対策概要

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 性質 | 代表的な脅威 | 主な原因 | 主な対策 | モニタリング |
| 機密性 | 情報窃取  情報漏洩 | 脆弱性を利用する攻撃  認証情報を悪用した不正アクセス | 脆弱性管理  アクセス管理 | 管理の確からしさと適切さの把握(ログ・資産・構成・設定・アカウント等)又は不正検出 |
| 完全性 | 不正アクセスによるデータ改ざん、消去 |
| 可用性 | 不正アクセスによるデータ破壊  システム停止 | 脆弱性を利用する攻撃  認証情報を悪用した不正アクセス  機器・ソフトウェア障害 | 脆弱性管理  アクセス管理  冗長構成 | 管理の確からしさと適切さの把握(ログ・資産・構成・設定・アカウント等)又は不正検出  運用稼働監視 |

脆弱性を利用する攻撃は、戦術、手法ともに多岐にわたり、また近年、攻撃手法の高度化から、詳細な検討は一般的に困難であると言わざるを得ない。しかし、セキュリティ上の不具合から情報漏洩等が発生したような場合は、ベンダーの契約不適合を問われる可能性がでてくる。そのため、民法改正WGの下部組織としてセキュリティ検討プロジェクトチームを設置し、セキュリティ専門家によるセキュリティ仕様を確定するための手法の検討を行った。

### 改正民法対応モデル取引・契約書に適したセキュリティガイドライン

システム開発関連契約における納品物において、セキュリティ上の不具合による情報漏洩等、その他重大なインシデントが発生したような場合は、ベンダーの契約不適合を問われる可能性がでてくる。その課題解決の一助とするべく、セキュリティ検討プロジェクトチームは、企業システムで広く使用されているWindows、Linuxを対象に、MITRE ATT&CK[[6]](#footnote-6)でまとめられたサイバー攻撃の戦術および攻撃手法をベースに、最近の攻撃に利用されている攻撃手法の実績や、攻撃者の観点から見た攻撃手法の利用頻度等を勘案した重み付けを専門家チームで絞り込み、それに対する具体的な対策や緩和策[[7]](#footnote-7)を整理した。また、それらの対策・緩和策に具体的な実装方法を盛り込むために、米国国防総省が提示しているSTIGsをはじめ、その他各ソフトウェアメーカーが提示するSTIGsに記述された内容と紐付けを実施することで、これまでにない脅威ベースによる実質的で具体的な対策・緩和策を示したセキュリティガイドラインを目指した。

A screenshot of a cell phone

Description automatically generated

表 ：脅威の重み付けと絞り込み

セキュリティガイドラインは、以下の特徴を持つ。

・MITRE ATT＠CKに記載された戦術・攻撃手法をもとに構成。

・基本的に、ATT&CKの改訂に応じて対応策や設定値を追加・修正。（バージョン管理）

・攻撃手法の実績や、攻撃者の観点から見た攻撃手法の利用頻度等を勘案しMITRE ATT＠CKの攻撃手法を絞り込み[[8]](#footnote-8)。

・対策・緩和策はSTIGs[[9]](#footnote-9)の内容を盛り込んだ具体的な実装方法を記載。

システム開発委託契約において、改正民法で一新される契約不適合に係る担保責任の規律に対応するためには、開発当時のセキュリティ水準に沿ったセキュリティ対策を施すことが重要となる。そのためには、可能な限り最新のサイバー攻撃に関する戦術・攻撃手法を反映した対策・緩和策を継続的に共有できる仕組みが必要であり、ユーザー・ベンダー間でセキュリティ仕様を適切に合意した上で開発業務を進めるための検討材料としてこのセキュリティガイドラインの利用を推奨する。また、システム開発委託契約において、開発当時のセキュリティ水準であることを合理的に明示する方法として、契約時点の最新のセキュリティガイドラインのバージョンをエビデンスに残すことを推奨する。これにより、納入後に発生したセキュリティ上の不具合による情報漏洩等、その他重大なインシデントが発生した場合でも、ベンダーの契約不適合が問われる可能性を低減できると考える。

## セキュリティ仕様検討プロセス

### 企画支援プロセス

企画支援プロセスの目的は、経営・事業の目的、目標を達成するために必要なシステムに関係する要件の集合とシステム化の方針および、システムを実現するための実施計画を得ることにある。このプロセスでは、ユーザーがベンダー候補者に対し、RFIを通してセキュリティガイドライン対応の可否に関する情報収集を実施することや、RFPによるセキュリティ要件の概要の明示がある。

＜ユーザー側＞

これまでの企画に関する慣例プロセスとしては、中期計画に基づいた当該システムに対する業務要件調査や分析を実施し、その実現に関連する情報を収集する手段としてRFIを提示する、いわゆるシステム化構想を具体的な案とすることである。さらに、RFIで収集した情報をもとに、当該システムの要件概要をRFPとして明示し、適切な提案ができるベンダーを絞り込む事で、ユーザー側の自社内体制を含めて、当該システムのシステム化計画を設定することであろう。

ここでは、セキュリティ仕様策定という観点で、このプロセスに適切なものとする組織の重要な仕組みは何であるかを考えたい。まず、事業に関連する法規制の明確化[[10]](#footnote-10)と、この規制対象となる業務に起因するリスク（サプライチェーンリスクを含む）、また事業継続計画を含むリスクマネージメントが運用され、リスク管理に関する業務要件が、RFI・RFPに反映さることが望まれる。

さらに、主にこの後のプロセスである要件定義や外部設計で参照する新セキュリティガイドラインについて「対応可能であるベンダーか否か」はRFIでベンダーを絞り込み、セキュリティガイドラインに基づくセキュリティ要件の概要をRFPで明示することが必要である。

一方、一部の技術レベルの高いユーザーにおいては、業務システムの調達・拡張・刷新において独自のセキュリティ仕様を実装する必要があり、ベンダーの支援を要せず、後述の(1) システム化構想、(2) システム化計画、(3)提案、 (5) システム要件定義まで、独自で実施した結果からの要件をRFPに記述し、それを実装可能とするベンダーを選定することが想定される。これはシステム開発業務全体の効率や見積精度、リスク管理などの観点から理想的である。

**(1)システム化構想**

経営上のニーズや課題を実現・解決するために、ユーザーが置かれた経営環境を踏まえて新たな業務の全体像の明確化とその実現をするためには、システム化構想および推進体制を立案することが必要である。RFIによりベンダーに対してシステム化構想と推進体制を明確に伝える事と同時に、セキュリティ要件の方針や概要を策定するために、セキュリティガイドラインへの対応可否に関する情報を収集することを念頭におく必要がある。ユーザーはセキュリティガイドラインにおける検討するべき脅威（攻撃手法）に対する対策や緩和策の実装に関する実現方法、運用方法、サプライチェーンリスク管理を含むセキュア開発に対応し、最適なソリューションが提案できるベンダーの選出を行う。

**(2)システム化計画**

セキュリティガイドラインへの対応可否情報が揃ったところで、絞り込んだベンダー候補者に対しセキュリティ要件概要を明示する。セキュリティ仕様を合意するためには、「守るべきものは何か」「どのように守るか」「費用対効果は適切か」という観点について、ベンダーとの間でNDAを締結した上で、適切に共有する必要がある。その時点で可能な範囲での当該システムに関連する、情報資産、IT資産、ネットワーク構成を含む構成設定管理情報を開示し、セキュリティガイドラインに基づいたセキュリティ要件の概要を明示する。

＜ベンダー側＞

当該システムに対し、ベンダーはユーザーに対しセキュリティガイドラインに基づくために必要な情報の提示要請と、条件の明記を適切に行う必要がある。このような提案業務を実施するためには、担当するシステムエンジニア（以下SE）のための標準を定め、周知することが望ましい。また、SEスキル管理や必要なリソース確保のための人材育成計画、これらを確実に実施するための中期事業計画が必要となる。

**(3)提案**

ユーザーへの提案では、NDAを締結した上でユーザーから提供された情報に基づき、リスク分析、技術的対策の検討、費用対効果を分かりやすく説明し、ユーザーのプロジェクトを成功に導くことが必要とされる。そのために、セキュリティガイドラインに基づくシステム開発の条件[[11]](#footnote-11)を提案書に記述し、要件定義作成支援プロセスの開始までにユーザーが準備することを促す。また、セキュリティガイドライン対応に関する情報の提示要請と条件の明記を促すことを推奨している。

### 要件定義作成支援プロセス

要件定義支援プロセスは、定義された環境において、当該システムの利用者及び他の利害関係者が必要とするサービスを提供できる要件を定義することを目的とする。ユーザーがセキュリティガイドラインを参考にしながら当該システムの情報セキュリティの要件定義書を作成する際は、必要に応じてベンダーの支援を得ながら完成させることを推奨する。

＜ユーザー側＞

企画支援プロセスで実施された当該システムの業務要件調査・分析結果から、さらに具体的な要件定義を作成する際に必要となるのは、当該システムのサービスにより向上する業務効率や付加価値創出のプラス面と、当該システムを導入することによって新たに追加されるリスクによるマイナス面とのバランスの検討である。このような検討は、情報セキュリティにおけるリスクコントロールとして、セキュリティガイドラインの戦術・手法において記述されている脅威と、それに対する対策・緩和策実装の検討により可能となる。

当該システムに関連する脅威の選定は、必要に応じてベンダーからのレクチャーを受けることを推奨するが、この脅威選定の精度をあげるには、当該システムにおけるインシデント発生時の影響に関して、リスクマネージメントや品質・セキュリティマネジメントで分析された情報（例えば、リスク低減対策、既存システムのセキュリティ対策、運用上の課題など）がベンダーに提供されることである。これにより、中期計画における経営・事業の目的、目標の達成に向けた事業コントロールが理想に近づく。

また、情報資産、IT資産、ネットワーク構成を含む構成設定管理情報は、その管理対象範囲、情報の精度、更新即時性等によって、セキュリティ対策・緩和策の選定、その効果、インシデント発生時のトリアージ、サイバー攻撃リスク受容の検討に直接影響するため、セキュリティ対策全体のコストが大きく変わることが考えられる。そのため、これらの情報は都度ではなく常に、品質・セキュリティマネジメントシステムの中で管理・計画・実施されることで、セキュリティ投資効果が高まる。

**(4)要件定義**

要件定義書には当該システムの機能要件を記述するほか、セキュリティ要件を検討するために提示するべき情報として、当該システムおよび当該システムに接続される既存システムの、情報資産、IT資産、ネットワーク構成を含む構成設定管理情報がある。

**情報資産：**

業務により入手、またはPCやシステムで作成したデータファイルがこれに当たる。要件定義の際にその存在を告知する資産の種類としては、要配慮個人情報や機微（センシティブ）情報（金融ガイドライン）等が含まれるデータファイルや、関連する個人情報を取り扱うすべての部署、担当者（パートやアルバイト、外注業者も含む）の入出力に関する権限（入力、閲覧、加工、出力）も含まれる。その他、営業情報など、インサイダー取引の対象となるもの、その関係者の入出力に関する権限等や、知財情報（漏洩や公開に伴う競争上のリスク、社会的被害や金銭的被害の検討結果など。）  
情報資産は可能な限り持たないことを念頭に置き、必要のない情報は物理的な資産を含め削除・廃棄することが望ましい。

**IT資産管理：**

IT資産管理は一般に、ハードウェア資産管理、ソフトウェア資産管理（部品表管理、ライセンス情報を含む）、構成設定管理（ソフトウェアが実装されているハードウェアとの紐付けや設定情報）、脆弱性管理の4つに分けられるが、ここでは次のシステム開発カテゴリに分類した方法を推奨する。システム開発カテゴリには、開発アプリケーション、利用コンポーネント（FOSSなど）、利用パッケージ、利用基盤に分けられ、それぞれに資産項目と管理項目において差があるため、ベンダーとのセキュリティ要件検討の際に参考にされたい。

表 3 システム開発カテゴリとIT資産管理項目

|  |  |  |  |
| --- | --- | --- | --- |
| システム開発カテゴリ | | 対象例 | IT資産管理項目 |
| 開発アプリケーション | | ベンダー開発アプリケーション | ・SW資産管理による使用許可 |
|  | 利用  コンポーネント | FOSS等 | ・SW資産管理（部品表、ライセンス等を含む）による使用の許可  ・最新の脆弱性情報との紐付け |
| 利用パッケージ | | CMS、フレームワーク等 | ・SW資産管理（ライセンス等を含む）による使用の許可  ・最新の脆弱性情報との紐付け  ・構成設定管理 |
| 利用基盤 | | OS、サービス、アプリケーション等 | ・SW資産管理（ライセンス等を含む）による使用の許可  ・最新の脆弱性情報との紐付け  ・構成設定管理 |
| ハードウェア | | PC、サーバー、モバイルデバイス、  NW機器、ストレージ、USB、IoT等 | ・HW資産管理（モジュールRev等を含む）による使用の許可  ・最新の脆弱性情報との紐付け  ・構成設定管理  ・ネットワーク構成 |

**ネットワーク構成を含む構成設定管理：**

セキュリティ要件検討には、既存システムを含んだ物理的に接続されているシステムの正確なネットワーク構成情報が必須となる。必要な範囲をベンダーと確認しながら共有し、モデル契約対応セキュリティガイドラインに記載されている戦術・手法に対して、想定外の経路からの攻撃や侵入を防止しなければならない。

・IPアドレス構成（セグメント単位）

・セグメントごとの許可されているプロトコル

・ルーティング情報

・Firewall設定

・VPN構成[[12]](#footnote-12)（セグメント、プロトコル、認証方式等）

・公開サーバー情報（公開プロトコル、制御接続方式、認証方式、DMZ構成等）

・重要資産を保存しているサーバー情報（IP、機微情報の有無、項目、暗号化の有無、保存方式）

・重要資産にアクセスする端末情報（IP、アクセスが許可される項目、ローカルの保存の有無、  
保存方式）

・その他、構成中や将来的に変更されるネットワーク構成も共有する。

＜ユーザーとベンダー間の協議＞

ベンダーは、ユーザーが提示した情報資産、IT資産、ネットワーク構成、設定管理状況をもとに、セキュリティガイドラインに記述された脅威（戦術・攻撃手段）を参考にして、不正アクセスを想定したセキュリティ対策範囲を定め、これを当該システムにおいて定義された環境とする。そして、利用者及び他の利害関係者が必要とするサービス提供を可能とする当該システムのセキュリティ要件を検討する。

＜ベンダー側＞

ユーザーから提示された情報をもとに、当該システムにおけるセキュリティ対策範囲の定義や、セキュリティガイドラインに基づいたセキュリティ要件の必要性を適切にレクチャーするために、担当するSEのための標準を定め、周知することが望ましい。また、SEスキル管理や必要なリソース確保のための人材育成計画、これらを確実に実施するための中期事業計画が必要となる。

### 外部設計作成（支援）プロセス

外部設計作成（支援）プロセスは、ソフトウェア方式設計プロセスと、ソフトウェア要件定義プロセスからなる。ソフトウェア方式設計プロセスは、実装した要件に対して検証できるソフトウェアの設計を提供することを目的とする。その要件としては、ユーザーとベンダーが協議したセキュリティ要件で実装することとした脅威に対する対策・緩和策であり、それが有効であることを検証できるソフトウェア設計を提供することが目的となる。さらに、ソフトウェア要件定義プロセスにおいては、ソフトウェア方式設計プロセスで設計されたシステムのソフトウェア要素の要件を確立することを目的とする。

＜ユーザー側＞

セキュリティ要件定義書に基づいたセキュリティ仕様書のドラフトを提示するために、セキュリティガイドラインにあるすべての設定対策に必要な措置を暫定要件として盛り込み、さらに「緩和策一覧」にある「緩和の方針」毎に、「緩和策実装」または、「リスクの受容」といった方針を明示する。リスクの受容に関してはユーザー側で具体的な攻撃シナリオがイメージできない場合が想定されるため、その場合はベンダーに相談することを推奨する。

**(5)システム要件定義**

ユーザーが提示したセキュリティ仕様のドラフトについて、ソフトウェア方式設計上の課題（実装することで機能要件を実現できない、または想定外のコストが上乗せされる、利用基盤のソフトウェア要素のバージョンにより対応不可、等）について協議を行う。この協議には脅威毎の「緩和策実装検討シート」を利用し、戦術毎に対策ポリシーを記述しエビデンスとして管理する。**【参考4：緩和策実装検討シート例】**

一部の緩和策の実装を諦めるとしても、当該脅威に関する攻撃シナリオで検討し、運用での緩和や他の緩和策による脅威の緩和を明示化する。その場合、コストの割り振りやリスク受容に関する決定についてユーザーの経営陣との合意を得る。

**デフォルト緩和策：**

セキュリティガイドラインの対策効果を有効にするため、ガイドライン以外に最低限実装するべき対策として「デフォルト緩和策」を策定した。**【参考5：デフォルト緩和策　端末編　＜一覧表＞】**、**【参考5：デフォルト緩和策　端末編　＜詳細＞】【参考6：デフォルト緩和策　セキュリティ仕様 ・Webアプリケーション編】**

デフォルト緩和策は、ユーザー・ベンダーが実装しなかった原因でインシデントが発生し、システムの利用者等に損害を被らせた場合に「重大な過失（重過失）」（ほとんど故意に近似する注意欠如の状態と解されるものや、わずかな配慮で注意義務を容易に尽くすことができたのであるから重過失があったというべきもの）や、「予見性」（実装しないことが原因でインシデントが発生すると予見できたもの）を問われる可能性がある対策である。[[13]](#footnote-13)

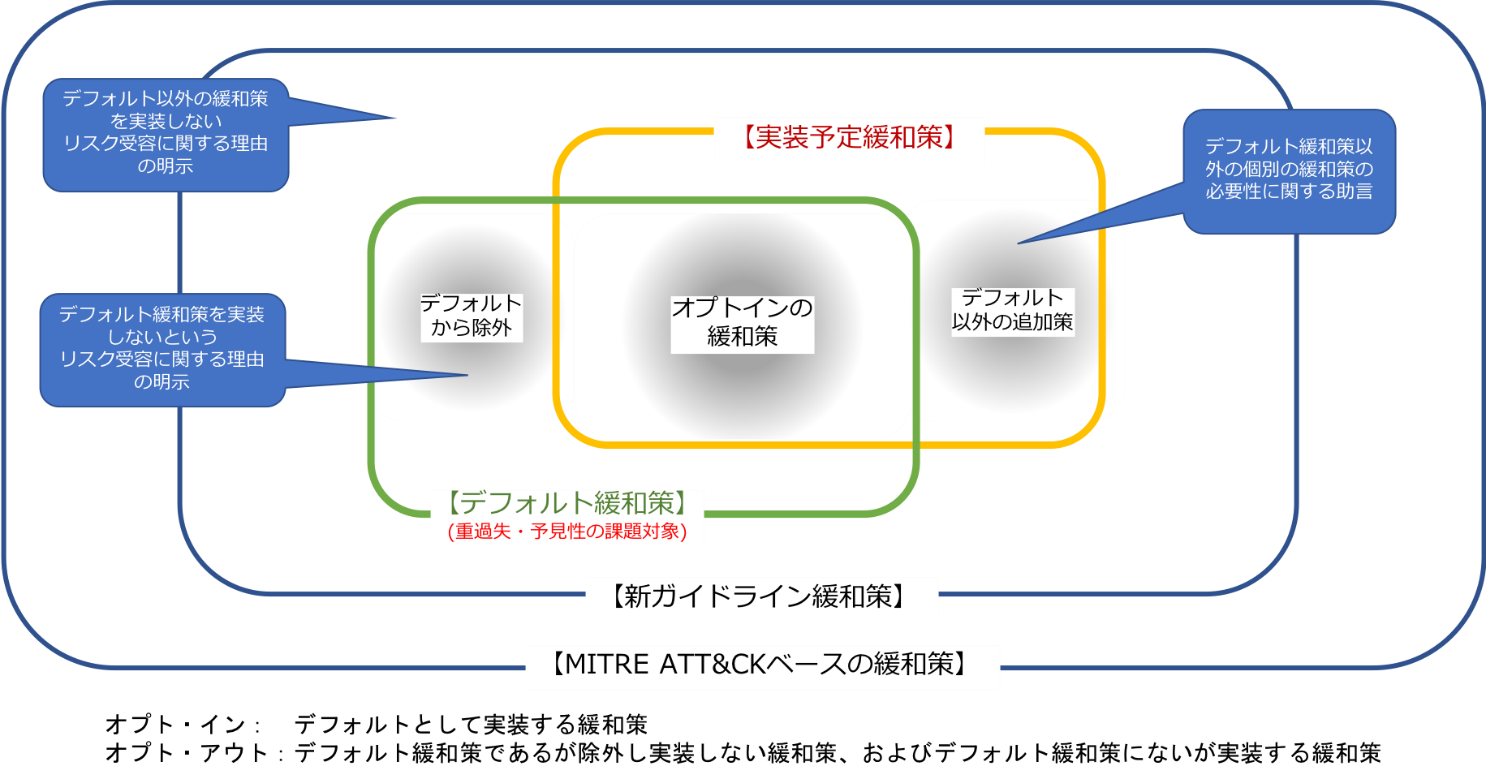


図 　デフォルト緩和策の位置付け

「参考5：デフォルト緩和策　端末編　＜一覧表＞」および「参考5：デフォルト緩和策　端末編　＜詳細＞」は、ユーザー主体による運用管理および業務ルールによる対策として実施することが想定されるが、システムによる自動化、制限機能、チェック機能等の実装または実施を促すような対策もあるため、必要に応じてシステム開発時のセキュリティ仕様として盛込むことも推奨する。また、この対策は、ガイドラインによるリスク低減の効果に大きく影響するため、ベンダーはユーザーに対して内容をレクチャーすることを推奨する。

「参考6：デフォルト緩和策　セキュリティ仕様・Webアプリケーション編」は、ベンダーがWebアプリケーションを受託開発する場合に、最低限実施するべきセキュリティ仕様である。

これらのデフォルト緩和策においても、ユーザーの業態、事業戦略、事業をとりまく環境等により、実装しない判断やデフォルト緩和策以外の緩和策を積極的に実装するべきものがあると考えられる。

セキュリティガイドラインやデフォルトとして含まれる緩和策から、実装予定緩和策を決定する際、以下のエビデンスが必要となる。

・デフォルト緩和策を実装しないというリスク受容に関する理由の明示（ユーザー）

・デフォルト緩和策以外の個別の緩和策の必要性に関する留意事項・改善案等の明示（ベンダー）

・デフォルト以外の緩和策を実装しないリスク受容に関する理由の明示（ユーザー）

＜ベンダー側＞

**セキュリティ設定：**

セキュリティガイドラインに基づく対策ポリシー（対策の実装、リスクの受容、他の対策による緩和）を決める際、ベンダーは当該システムを想定した攻撃シナリオやインシデント事例を用いてレクチャーし、脅威に関する認識をユーザーと共有した上で、サーバー設定やグループポリシー等、対策の一環となる利用コンポーネントの設定、もしくはセキュリティ製品の導入をユーザーと検討する。

検討に当たっては、重要資産防御における費用対効果、納期、運用、保守を勘案し、効果が少ないと考えられる場合は、暗号化等の運用を検討し、実質的な被害低減によるリスク受容を含めユーザーと検討する。

**FOSS脆弱性管理：**

システム開発においては、開発業務効率や即時対応を重視するため、またコスト削減を目的に、ユーザーの指定によりFOSSを使用し開発することが主流になっている。しかし、ユーザーから指定されたFOSS以外、ベンダーが開発しているシステムにどのようなFOSSを採用しているかを明示することには消極的である。加えて日本の多重下請け構造では、どこでどのようなFOSSが利用されているかを把握するのが難しく、ソフトウェアのサプライチェーンリスクも懸念される。**【参考7：汚染される開発環境】**

FOSSの脆弱性管理を実施するには、第一に自社のFOSSの使用状況を把握することにある。そして、使用するコンポーネントが、インターネット上に公開されているFOSSの脆弱性情報と照らし合わせ、個々の脆弱性に関する詳細な情報や深刻度を把握すること推奨する。

**使用するコンポーネント：**

外部設計において使用するコンポーネントを明示する。FOSS脆弱性管理によるサプライチェーンリスクの回避とともに、将来的に顕在化の可能性のある脅威についてトレーサビリティを確保するために、使用するコンポーネントの部品表を提示する。部品表としてはSoftware bill of materials (SBoM) を推奨するが、情報の項目としては以下を参考とされたい。

・モジュール名

・バージョン、リビジョン

・取得先（リポジトリ）

・ライセンス種類

・委託先名、プロジェクト名、オーナー名等

・FOSS以外のコンポーネント[[14]](#footnote-14)に関しては、脆弱性の発生時やEoLの際の対応に関する記述、

　および有償保守、無償対応等の明記

**変更管理：**

システム要件定義により納期や見積額が決定した後で、セキュリティガイドラインの更新（利用基盤および利用パッケージにおける新規の脆弱性に対する緩和策の変更や追加など）や利用コンポーネント、利用パッケージ、利用基盤の脆弱性対応が遅れた場合に、納期変更やAPI変更に起因する開発費の再見積の必要性が出ることがある。このようなセキュリティの脆弱性発覚による変更管理が必要であることを予めユーザーに認識してもらう。

### ソフトウェア開発業務プロセス

ソフトウェア開発業務プロセスは、(6)ソフトウェア詳細設計、(7)ソフトウェア構築、(8)システム結合、からなり、外部設計書およびセキュリティ仕様書に基づいてソフトウェア開発を実施するプロセスである。ベンダーはこれらのプロセスにおいて、知財・ライセンス管理、部品表管理、開発業務委託業者品質管理、FOSSや関連OSおよび利用コンポーネントの脆弱性管理を実施し、それらの管理と運用に関する業務ルールの励行について開発基準として定め、周知、教育を実施する。

＜ベンダー側＞

**(6) ソフトウェア詳細設計プロセス**

ソフトウェア詳細設計プロセスは、ソフトウェア要件及びソフトウェア方式に対して実装し、検証でき、コーディング及びテストを可能にするために十分に詳細である設計をソフトウェアの為に提供することを目的とする。外部設計およびセキュリティ仕様書に基づくソフトウェア開発を実施する際、その他の要件としてセキュア開発を実施することを推奨する。セキュア開発のセキュリティ要件概要を以下に示す。**【参考8：セキュアコーディングガイド】**

このセキュア開発セキュリティ要件概要もユーザーと共有し、また、詳細設計方針として合意して内部設計書として管理する。

**(7) ソフトウェア構築プロセス**

ソフトウェア構築プロセスは、ソフトウェア詳細設計プロセスで作成した内部設計書を適切に反映した実行可能なソフトウェアユニットを作り出すことを目的とする。成果物のプログラムは部品表とともに管理する。

**(8)システム結合プロセス**

システム結合プロセスは、システム設計及びシステム要件に表現された顧客の期待を満たす完全なシステムを作り出すためにシステム要素（ソフトウェア構成品目、ハードウェア構成品目、手作業及び必要に応じて他のシステム）を結合することを目的とする。

### ソフトウェア運用準備移行支援業務プロセス

このソフトウェア運用準備移行支援業務プロセスは、(9)システムテスト、(10)導入・受入支援、(11)運用テストからなり、本番稼働となる運用業務プロセスへの最後のプロセスであると同時に、サイバー攻撃の隙が生じるプロセスでもある。

サイバー攻撃事案における重大なインシデントとして、旧システムから新システムへの切替期間または併用期間において、また切り替え期間が終了した後であってもネットワークアクセス制御や認証システムの切り替えミスや忘れによって攻撃されるというケースが散見されるため、(9)(10)(11)のプロセスで必要となるルーティング条件や認証条件の緩和、アクセス特権の複数人での共有などの設定は、これらプロセスが完了した時点で、本番稼働設定に確実に切り替えなければならない。また、バックアップ、リストアの際の復元条件を明確にすることも重要である。

**(9)システムテスト**

各システム要件について、実装の適合性がテストされ、システムの納入準備ができていることを確実にすることを目的としている。

**(10)導入・受入支援**

合意した要件を満たすシステムを実環境に導入し、システムが要件を満たしているという確信を取得者が持つことを助けることを目的とする。

**(11)運用テスト**

ハードウェア製品またはサービスとして実現される指定のシステム要素を作り出すことを目的としている。

### 運用業務プロセス

意図された環境でシステム及びソフトウェア製品を運用し、システム及びソフトウェア製品の顧客への支援を提供することを目的とする。企画支援プロセスにおいて計画された、経営・事業目的・目標に適合した

SLAに基づき、サービスレベル維持に必要な運用・保守に関連する契約を締結する。また、セキュリティ監視やCSIRTとの連携がある場合は、インシデント発生時の対応体制や役割に関する文書を更新する。

## 【参考1：セキュリティ策定の現状と課題】

### 参考 1.1 サイバー攻撃の現状

情報通信研究機構（NICT）のデータによれば、観測する約30万IPアドレスにおいて合計2121億パケットのサイバー攻撃関連の通信が確認されており、1 IPアドレス当たり約79万パケットが届いている。

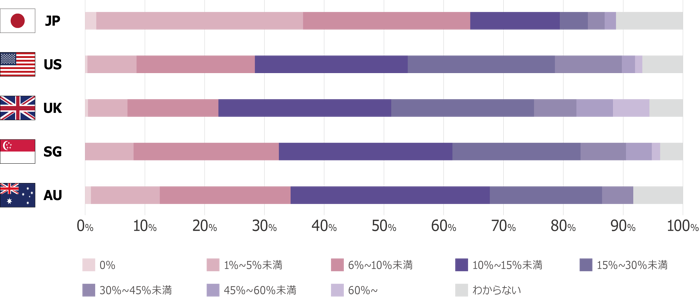
A screenshot of a cell phone

Description automatically generated（出典元URL）[https://www.nict.go. jp/press/2019/02/06-1.html](https://www.nict.go.jp/press/2019/02/06-1.html)

参考＿図 ：NICTERダークネット観測統計（過去10年間）

また警察庁の発表によれば、IDやパスワードの窃取を目的とした不正アクセス禁止法違反の検挙件数は564件（2018年）、情報窃取を企図した標的型メール攻撃は2,687件（2019年上半期）発生するなど、サイバー攻撃の発生や被害は後を絶たないのが現状である。さらにはサイバー攻撃の一つの原因ともいえる脆弱性は、2018年の年間で16,314件（CVE数）確認されており、情報処理推進機構（IPA）に届け出が行われた件数はソフトウェア製品とウェブアプリケーションの脆弱性を合算すると約55,000件の届け出が行われている。

一方で組織側のサイバーセキュリティ意識は未だに低いのが現状である。例えば、日本情報システムユーザー協会（JUAS）の調査によればCISO（セキュリティ担当役員）の設置する企業は約2割に留まり、約7割は未検討となっている。またNRIセキュアテクノロジーズの調査によれば、IT関連予算に占めるセキュリティ予算の割合で、10%以上をセキュリティ関連予算に充てている企業は約２割しかないが、アメリカやイギリスでは約６～７割を占めている。経営層の関与や予算の付与などからもサイバーセキュリティが経営課題として認識されていない現状があると言わざるを得ない。



参考＿図 ：セキュリティ関連予算の割合

（出典元URL）<https://www.secure-sketch.com/blog/insight2018-security-management>

A screenshot of a cell phone

Description automatically generatedまた昨今のサイバー攻撃はシステムやサービスの利用時に侵入するものだけではなく、より早い段階から侵入されているケースも確認されている。例えば、出荷前の端末にマルウェアが混入していたり、ソフトウェアを開発する開発環境そのものが汚染されていたりするなど、サイバー攻撃が行われるフェーズもより早くなっている。さらには設計上の不備や設定ミスなどからサイバー攻撃を自ら招き入れてしまい、インシデントが発生しているケースも多数みられる。

参考＿図 ：開発段階のセキュリティ方針・基準の有無

（出典元URL）<https://www.ipa.go.jp/files/000065094.pdf>

インシデントがより早い段階で発生しているにもかかわらず、IPAの「IoT 製品・サービス開発者におけるセキュリティ対策の現状と意識に関する報告書」の調査結果によると、開発段階のセキュリティ方針・基準を設けている企業は4割にも満たず、設計や開発フェーズにおけるサイバーセキュリティ対策の軽視ともみられる結果も出ている。

改正民法に伴い、これまで以上に発注者側と受注者側の双方が組織内外の利用システムや製品やサービスの開発や提供にあたって、サイバーセキュリティに関する議論を深めておく必要がある。引き渡しを行った時点でどのようにセキュリティ対策を行っていたのかを適切に証明できなければ、消滅時効10年の間に組織間のトラブルに発展しかねない状況にある。サイバーセキュリティは導入やリリース前の検証のフェーズから開始するのではなく、企画や設計の段階から対策を鑑みてプロジェクトを推進する必要がある。適切に検討が行われなければ、契約者間のいずれの組織も資源や機会の損失を招く恐れがあることは忘れてはならず、前もってサイバーセキュリティに関する議論を深め、リスクがある場合はどのようなリスクを受容し、事業の継続を行っていくのかを検討しなければならない。

### 参考1.2 サイバーセキュリティに対する法規制

#### 1.2.1日本の関連法

日本においてサイバーセキュリティに関する法律は、刑法や民法、不正アクセス禁止法、さらにはサイバーセキュリティ基本法などが存在する。

|  |  |
| --- | --- |
| 法律 | 概要 |
| サイバーセキュリティ基本法 | 日本のサイバーセキュリティの基本理念や戦略、施策の基本を定めた法律。また同法でサイバーセキュリティの定義や国、地方公共団体重要社会基盤事業者、サイバー関連事業者、教育研究機関の責務や国民の努力などについて定めている。 |
| 不正アクセス禁止法 | 電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序を維持する等のために設けられた法律。不正アクセス罪をはじめ、不正な取得や助長、保管や入力要求などの不正に罰則が設けられている。 |
| 不正競争防止法 | 事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を定めた法律。2018年には限定提供データの不正取得等の禁止や技術的制限手段の保護の強化などの改正が行われている。 |
| 刑法 | 日本における犯罪や刑罰に関する法律。サイバーセキュリティ関連として、電磁的記録の不正作出及び供用、不正指令電磁的記録の作成や取得、わいせつ物頒布や電子計算機損壊等業務妨害、電子計算機使用詐欺などが定められている。 |
| 民法 | 日本における私法の一般法について定め、公権力を有さない組織や個人間の関係を定めた法律。2020年の法改正によって、瑕疵担保責任が契約不適合に改正されるなど、システム開発などの契約に関する債権法も含まれる。 |
| 著作権法 | 知的財産権である著作権について定めた法律。2018年の改正でプログラムのリバースエンジニアリングを可能にするなど、開発やセキュリティ運用等においても関連する。 |

#### 1.2.2海外の法制度

また昨今ではGDPRを始めとしたプライバシー関連の法律や諸外国で作成されているサイバーセキュリティ法においても、国内の組織に影響を及ぼしかねない法律が設けられている。

|  |  |
| --- | --- |
| 国 | 法律 |
| アメリカ | ・Cybersecurity Information Sharing Act  ・SB-327 Information privacy: connected devices. (State of California) |
| EU | ・The EU Cybersecurity Act ・General Data Protection Regulation |
| 中国 | 中华人民共和国网络安全法 |
| シンガポール | ・Cybersecurity Act 2018 ・Personal Data Protection Act 2012 |
| タイ | ・Thailand Cybersecurity Act ・Thailand Personal Data Protection Act |
| ベトナム | Luật an ninh mạng |

## 【参考2：SQLインジェクション事件（東京地裁平成26年1月23日判決）】

#### ※出典・引用元：日本シーサート協議会

Y社は、X社の販売サイトの構築および運営を受託していたところ、外部から不正アクセス（SQLインジェクション攻撃）を受け、7316件のクレジットカード情報を含む9482件の個人情報が漏えいした。

X社は顧客への謝罪関係費用から売上損失等の1億円余りの損害賠償を委託契約の債務不履行に基づきY社に請求した。

|  |  |
| --- | --- |
| 時期 | 説明 |
| H18.2.20 | 経産省は「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」と題する文書を公表 |
| H19.4頃 | IPAは「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」を公表 |
| H21.1.30 | X社とY社は、X社を委託者、Y社を受託者とする業務委託に係る基本契約を締結 |
| H21.2.4 | Y社に対し注文書を交付し、注文を発注した |
| H21.4.15 | Webサイトの稼働開始 |
| H22.1.26 | X社がY社に対し機能カスタマイズを発注 |
| H22.1.29 | 機能カスタマイズされたシステムを稼働 |
| H23.4.14 | 不正アクセス、7316件のクレジットカード情報を含む9482件の情報漏えい |

平成18年2月20日、経済産業省は、「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」と題する文書において、SQLインジェクション攻撃によってデータベース内の大量の個人データが流出する事案が相次いで発生していることから、IPAが紹介するSQLインジェクション対策の措置を重点的に実施することを求める旨の注意喚起をしていた。また、IPAは、平成19年4月、「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」と題する文書において、Webアプリケーションに対する代表的な攻撃手法としてSQLインジェクション攻撃を挙げ、バインド機構の使用またはエスケープ処理を行うこと等により、SQLインジェクション対策をすることが必要である旨を明示していた。

これらのことから、Y社がX社との間で、本件システム発注の契約を締結した平成21年2月4日において、本件データベースから顧客の個人情報が漏えいすることを防止するために、SQLインジェクション対策として、バインド機構の使用またはエスケープ処理を施したプログラムを提供すべき債務を負っていた。

にもかかわらず、Y社は、本件Webアプリケーションにおいて、バインド機構の使用およびエスケープ処理のいずれも行われていなかった部分があることから、Y社の債務不履行が認められる。また、第三者がSQLインジェクション攻撃を行うことにより本件データベースから個人情報が流出し得ることはY社において具体的に予見可能であり、それを超えて、個別の侵入態様を予見できなかったとしても、債務不履行に係るY社の予見可能性は否定されない。

一方、X社は、クレジットカード情報がデータベースに存在し、セキュリティ上はクレジットカード情報を保存しない方が良いと認識し、Y社からもクレジットカード情報を保存しない方法の提案を受けたが、X社はこの提案を採用しなかったため、X社に3割の過失が認められ過失相殺された。

結局、認定された損害である3231万9568円の3割を過失相殺によって控除し、2232万3697円の損害賠償金を支払うよう命じた。 なお、X社とY社との間で締結された契約には、賠償金額の制限条項が存在したが、Y社に重過失が認められたため、同条項は適用されなかった。

**【SQLインジェクション事件に関するコメント】**

本事案は、ユーザーであるX社がベンダーであるY社からなされたシステム改修の提案（クレジットカード情報を保存しない改修）に対して沈黙するなどリスクコミュニケーションの不全が一因であり、セキュリティ仕様について、ユーザー・ベンダー間が誠実に検討することが望まれる。

また、本事案では、発注契約を締結した当時の技術水準において、SQLインジェクション攻撃による個人データ流出事案が相次いでおり、バインド機構とエスケープ処理といったSQLインジェクション対策を講じなければ個人情報が流出し得ることがベンダーにも予見できたと述べられている。このセキュリティ仕様策定プロセスにおいては、システム仕様が一旦確定した以降は、システム仕様に従って開発工程の作業を遂行すれば契約不適合責任を負わないことを原則としているが、確定されたシステム仕様が契約当時の技術水準に照らしてセキュリティに係る脅威に対する対策として不十分であり、これがベンダーにとって予見可能であった場合には、ベンダーはユーザーに危険があることを告げて適切なシステム仕様となるように留意事項・改善案等を明示するなどの説明義務を怠ったものとされる可能性があるものと考えられる。なお、本事案においては、ベンダーが「クレジット情報の保存による危険性を説明したといえる」などとしてベンダーの説明義務違反については認定されていない。

本判決では、バインド機構とエスケープ処理といったSQLインジェクション対策を超えるデータベースの暗号化処理などについては、ベンダーの債務とされていない。もっとも暗号化処理がベンダーの債務となるか否かは、契約当時の技術水準にも左右されるが、単に技術水準だけではなく、ソフトウェアの利用目的及び利用環境等に加えて、セキュリティ仕様を策定するプロセスにおけるユーザーのリスク受容の判断の有無及び当該判断に至るベンダーの説明が信義則上も相当であるかどうかなどによっても左右されるものと考えられる。

## A close up of a map Description automatically generated【参考3：セキュリティ仕様策定プロセスイメージ図】

## 【参考4：緩和策実装検討シート例】



戦術毎に緩和策の方針を参考に

対策ポリシーを記述する。

・実装する対策・緩和方法

・リスク受容する

・他の戦術に対する対策・緩和策で

　リスク低減する。

## 【参考5：デフォルト緩和策　端末編　＜一覧表＞】

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **前提事項** | | サポート切れソフトウェア（OS・アプリケーション）は使用していないことが前提です。利用者はサポート内（できる限り最新のバージョンの）製品を利用し、最新のパッチが適用されたソフトウェアを利用し、ソフトウェアの推奨指定されている機能については出来る限り利用するように心がけましょう。 | | | | | |
| **No** | **項目** | | **概説** | **期待できる効果** | **考えられる影響** | **影響の緩和策** |
| 5-1 | 教育の実施 | | 経営者向け：サイバーセキュリティ経営のリーダーシップをとり、セキュリティマネジメントのための知識を身に着ける。 | 適切な投資（セキュリティ対策費とリスク受容のバランス）の実施 | 具体的な方法がわからない | IPA 中小企業の情報セキュリティ対策ガイドラインの活用 |
| セキュリティ設定の重要性や運用の必要性を理解し、指示・対応可能な知識を身に着け、継続的に組織に対して脅威情報などのインプットを行う。 | インシデント発生時の対応、社内外への適切な運用の維持、注意喚起の実施 | 具体的な方法がわからない | IPA 中小企業の情報セキュリティ対策ガイドラインの活用 |
| 従業員向け：設定の意味や運用の背景を理解する | 最新の攻撃手口の習得、適切な運用と報告 | 集合教育が難しい、コンテンツがない | IPA コンテンツの活用 |
| 5-2 | 重要情報資産の暗号化とバックアップの実施 | | 重要資産を指定し、暗号化を行い、定期的にバックアップをとる。 | 被害の軽減／復旧 | バックアップシステムの導入コスト | クラウドの活用（OneDrive、GoogleDrive、DropBox） |
| 5-3 | 管理者権限の制限 | | 利用者にローカルの管理者権限を付与しない （特権IDの適切な管理）。 | 特権昇格・永続化の防止／資格情報の窃取の防止 | アプリケーションインストールが不便 | インストール時のID/パスフレーズの付与 |
| 5-4 | アンチウイルス製品の利用 | | パターンファイルの更新、クイックスキャン(日次)・完全スキャン (週次)の実施。 | 初期侵入の軽減／マルウェアの実行の防止 | スキャンが重く、PCが遅くなる | SSDへの換装（業務効率も向上） |
| 5-5 | 修正プログラムの適用 | | 脆弱性を修正するプログラムがリリースされた場合は、リリース後速やかに適用する（対応が難しい場合は代替策を用いる）。 | 初期侵入の軽減／マルウェアの実行の防止 | アプリケーションが動かなくなる | ベンダー情報の収集、互換性の低いアプリの運用停止 |
| 5-6 | マクロ・スクリプト禁止と保護ビューの利用 | | Office、Acrobat製品等のマクロを禁止し、保護ビューを設定し、外部からのファイルは保護ビューを解除しない。 | 初期侵入の軽減／マルウェアの実行の防止 | マクロが使えない | マクロ実行用バッチファイルの設定 |
| 5-7 | メール・ブラウザーの適切な利用 | | メールのファイルやリンクはむやみにクリックしない、リンク先を確認する、HTTPSで始まらないサイトは閲覧しない、ID/パスワードをブラウザーに保存させない、お気に入りは定期的に整理する。 | 初期侵入の軽減／マルウェアの実行の防止 |  |  |
| 5-8 | 多要素認証機能の利用 | | 顔認証や指紋認証、トークンなどを利用する。 | 資格情報の窃取の防止／水平展開の防止 | 設定がわからない | 専用サイトへの誘導 |
| 5-9 | セキュアなネットワークの利用 | | フリーWi-Fi（特にパスワード設定のないWi-Fi）は利用せず、テザリングを活用する。httpsのみの接続が望ましい。退職者が出た場合、Wi-Fiのパスワードを変更する。 | 初期侵入の軽減／資格情報の窃取の防止／水平展開の防止 | 見分け方がわからない | IPA コンテンツの活用 |
| 5-10 | 外部記憶媒体の利用制限 | | USBやスマートフォンなどの外部記憶媒体で顧客とデータ交換をしない。利用する場合は最新のアンチウイルス製品で完全スキャン後に利用する。 | 初期侵入の軽減／マルウェアの実行の防止 | 顧客とのコミュニケーションや対応が悪くなる | 社内規程を整備し、社内ルールであることを周知する |
| 5-11 | 適切に管理・設定されたパスワードの利用 | | 初期パスワードの変更（OS、ネットワーク機器等）を行い、端末・サーバーのローカル管理者のパスワードをユニークにする。またパスフレーズを活用し、設定する。 | 資格情報の窃取の防止／水平展開の防止／被害の軽減 | 設定がわからない | 導入業者に指示し、報告を受ける |

## 【参考5： デフォルト緩和策　端末編　＜詳細＞】

### ここでは、ユーザー主体による運用管理および業務ルールによる対策として実施することが想定されるが、システムによる自動化、制限機能、チェック機能等の実装または実施を促すような機能による対策もあるため、必要に応じてシステム開発時のセキュリティ仕様として盛込むことも推奨する。また、この対策は、ガイドラインによるリスク低減の効果に大きく影響するため、ベンダーはユーザーに対して内容をレクチャーすることを推奨する。

### 参考5.1 教育の実施

**実施対策**

* 1. サイバーセキュリティの維持のためには、IT部門・担当者に依存することなく、全社的な取り組みが必須である。サイバーセキュリティ経営を実現するために組織の役割に応じた教育を実施する。
     1. **経営者向け：**リーダーシップをとってサイバーセキュリティ経営を促進するためにセキュリティマネジメントの知識を身に付ける
     2. **中間管理職向け：**セキュリティ設定の重要性や運用の必要性を理解し、指示・対応可能な知識を身に着け、継続的に組織に対して脅威情報などのインプットを行う
     3. **従業員向け：**設定の意味や運用の背景を理解する

＜コンテンツ＞

* + 1. ・組織の情報資産を守れ！-標的型サイバー攻撃に備えたマネジメント-
    2. ・見えざるサイバー攻撃 -標的型サイバー攻撃の組織的な対策-
    3. ・そのメール本当に信用してもいいんですか？　-標的型サイバー攻撃メールの手口と対策-
    4. ・今　制御システムも狙われている！ －情報セキュリティの必要性－
    5. https://www.ipa.go.jp/security/keihatsu/videos/index.html

### 参考5.2 重要情報資産の暗号化とバックアップの実施

### 設定・運用対策

* 1. 組織内で重要情報資産を定義する。
     1. 情報の内容の識別：個人情報、機微情報、営業情報、技術情報、財務情報等
     2. 情報の機密度の識別：極秘、営業秘密、秘密、社外秘
     3. 情報の共有の識別：社内関係者限り、部門限り、関係部門間限り、社外を含む関係者限り、一般公開可能
  2. 定義に応じて、重要情報資産へのアクセス設定を行い、その上で暗号化する、しないを決定する。
  3. 情報資産の内容に応じて、バックアップの可否、バックアップの実施タイミング（日次、週次、月次、年次等）を決定し、実施する。

### 攻撃の手口

* 1. ゼロディ攻撃や、修正プログラムリリース前に攻撃コードが公開された場合で、アンチウイルスを始めとする緩和策がまったく有効でない場合がある。
  2. また、ランサムウェアに感染すると、データを暗号化されてしまうだけでなく、情報を窃取し、身代金を支払わない場合、窃取した情報をインターネットに公開するなどの手口も出現している。

### 現状の課題

* 1. データが窃取された場合、情報公開や悪用される可能性があり、事業継続に多大な影響を及ぼす可能性がある。ランサムウェアの場合、身代金を支払っても、データが復号できる保証はない。

### 対策の効果

* 1. 攻撃されることを前提に措置を講じることは、極めて有効である。
  2. 重要資産の暗号化は、情報漏洩の際に実質的な漏洩を軽減する効果があり、Zip暗号化やOffice文書のパスワード設定等で容易に設定が可能である。
  3. バックアップは、ランサムウェアなどの改ざんを行うマルウェア対策として極めて有効である。

### リスクの受容

* 1. 万一、マルウェアに感染し、データの暗号化等が実施された場合の復旧コストに比べ、はるかに低コストで防御が可能となるため、暗号化、バックアップを実施しないというリスク受容は推奨できない。

### 対策による弊害の緩和

* 1. バックアップ先として、Dropbox、Google Drive、OneDrive、VOX などの、ファイルの世代管理を実施するクラウドシステムがあり、情報資産の機密性、重要に応じて、これらの活用も視野に入れるべきである。（ランサムウェアで暗号化される前の世代のファイルで復旧できる）
  2. OneDriveの場合、マイドキュメント、デスクトップを自動的に随時、バックアップする機能がある。

### 参考5.3 管理者権限の制限

### 設定・運用対策

* 1. 管理業務以外の一般業務に携わる利用者には、管理者権限を付与せず、最小限の権限のみ与える。
     1. Windows においては、Built-in Administrators に利用者やドメインユーザーを所属させない。

### 攻撃の手口

* 1. マルウェアが、永続性の確保や、アンチウイルスの無効化、改ざん、情報漏洩といった実害を引き起こすためには、管理者権限が必要となる場合がある。

### 現状の課題

* 1. 利用者に管理者権限を与えている場合、マルウェアは侵入と同時に管理者権限で様々な行動が可能になり、新たなマルウェアをインターネットから呼び込んだり、C&Cサーバーと通信し、情報を外部に送信するなどの被害が発生する可能性が高まる。
  2. また、管理者権限であれば、アンチウイルスソフトの停止や、様々なセキュリティ設定を変更でき、監査証跡も消去が可能で、他の端末への拡散も実行可能となる。

### 対策の効果

* 1. 一方、標準ユーザーの場合、アプリケーションのインストール、OS やアプリケーションの設定変更が不可能であり、都度、管理者のID、パスワードが必要である。このため、特権昇格を試みている間に、検出が可能になる可能性が高まり、また、水平展開が困難となるなど、被害拡大を緩和できるメリットが大きい。

### リスク受容

* 1. 運用に弊害が発生するとの理由から、リスク受容することは危険であり、推奨できない。

### 対策による弊害の緩和

* 1. アプリケーションのインストール、設定変更のための個別のユニークなBuilt-In Administrators の ID、パスワードを PC に保存しないこと、適切な管理を前提に、標準ユーザーに印刷物で付与し、運用することを強く推奨する。

### 参考5.4 アンチウイルス製品の利用

### 設定・運用対策

* 1. アンチウイルスは端末、サーバー起動時にパターンファイルもしくはアンチウイルスソフト自体のバージョンアップを実施する。
  2. 日次1回は、マイドキュメント等のクイックスキャンを実施する。
  3. 週次1回以上、接続されたメディア全体の完全スキャンを実施する。

### 攻撃の手口

* 1. マルウェアは、アンチウイルスの検知を逃れるために、大量の亜種を作成する。亜種が多ければ多いほど、対応するパターンファイルのリリースに一定の時間がかかるためであり、この間に攻撃を完了しようという戦術に基づく。

### 現状の課題

* 1. 未対応のパターンファイルの場合、検出が困難であり、対応するパターンファイルのリリースまでの期間（delta）はマルウェアの侵入を許してしまう。

### 対策の効果

* 1. パターンファイルの更新、日次でのマイドキュメントへのクイックスキャン、週次での完全スキャンを実施することで、最新のパターンファイルでの検出ができる可能性が高まる。

### リスク受容

* 1. 完全スキャンについては、動作が遅くなる等の弊害も指摘されるが、最新のパターンファイルですべてをスキャンすることは、極めて重要であり、実施しないことで、マルウェアの活動を許す期間が長くなるため、このリスク受容は推奨できない。

### 対策による弊害の緩和

* 1. ハードディスクなどの低速のI/Oを使用している場合、完全スキャンはシステムの動作が緩慢になり、生産性が落ちる。一方で、SSDに換装することで、完全スキャンの弊害は回避できる上、起動や処理全般の高速化による生産性の向上も期待できる。

### 参考5.5 脆弱性修正プログラムの適用

### 設定・運用対策

* 1. 脆弱性修正プログラムは、リリース後、早期に適用する。
  2. テスト期間中や、適用が早期に行えない場合は、脆弱性の性質に応じた適切な緩和策を実施し、監査を強化する。

### 攻撃の手口

* 1. マルウェアは、OSやアプリケーションソフトの脆弱性を利用し、自身のインストールや永続性の確保を行う。

### 現状の課題

* 1. 修正プログラム適用によって、アプリケーションが動作しない等の理由で、修正プログラムの適用を実施できない場合がある。また、テストの工数負担が大きくすぐに適用できない場合や、運用上、システムを再起動できない24/365システムが存在する。

### 対策の効果

* 1. 脆弱性情報発表の数日後に、その脆弱性を利用する新種のマルウェアが出現するなどの実績があり、早期適用は強く推奨される。

### リスク受容

* 1. リスク受容する場合は、脆弱性の性質とシステムの特性に応じて、アクセス制限、不要なポートの遮断、脆弱性を有するプロトコルやアプリケーションの使用制限などの緩和策を速やかに実施し、監査を強化し検出に努める。

### 参考5.6 マクロ・スクリプト禁止と保護ビューの利用

### 設定・運用対策

* 1. Office のマクロは警告を発して原則禁止とする。保護ビューの設定を行う。
  2. PDF のスクリプトは原則禁止とする。サンドボックスによる保護（表示は、「保護されたビュー」）の設定を行う。
     1. [環境設定]>[Java Script]>[Acrobat JavaScript を使用] のチェックボックスを外す。
     2. [環境設定]>[Java Script]>[JavaScript のセキュリティ]>[メニュー項目の JavaScript 実行権限を有効にする] のチェックボックスを外す。
     3. [環境設定]>[セキュリティ(拡張)]>[サンドボックスによる保護]>[保護されたビュー]>[すべてのファイル] を選択。

### 攻撃の手口

* 1. ローダーと呼ばれるマルウェアは、Office文書、PDF文書に埋め込まれたマクロやスクリプトであり、文書を開かせることで起動する。起動後、ローダーは外部から新たにマルウェア本体をダウンロードする。このように複雑な手順を踏むのは、アンチウイルスによる検出を避けるためである。

### 現状の課題

* 1. 業務でマクロ・スクリプトを実行できる環境では、悪意ある文書の保護ビューを解除すると感染してしまう。

### 対策の効果

* 1. 業務でマクロ・スクリプトを実行しない環境では、出荷時規定値であるマクロ・スクリプトの禁止を維持し、保護ビューを解除しないことで、被害を緩和できる。

### リスク受容

* 1. 多くのマルウェアは、この攻撃手口を利用することから、リスク受容は推奨できない。また、マクロ・スクリプトの利用許可は、一種の脆弱性の容認であることから、文書化し、監査を強化することを推奨する。

### 対策による弊害の緩和

* 1. 業務でマクロ・スクリプトを実行する環境では、通常は、レジストリ設定でマクロ・スクリプトを禁止しておき、マクロ・スクリプト使用時のみ、レジストリを許可設定に変更したのち、マクロ・スクリプトファイルを使用する。使用後は、マクロ・スクリプトを禁止設定とする。一連の手順をバッチファイルにして、バッチファイルの操作で完了するようにする。

### 参考5.7 メール・ブラウザーの適切な利用

### 運用対策

* 1. HTTPSで始まらないサイトの閲覧、ダウンロードを禁止する。
  2. 電子メールに埋め込まれたWebサイトのリンクをクリックする場合は、実際のリンクを確認し、フィッシングサイトでないことを確実に確認する。HTTPS で始まらないリンクの場合は、送信者に確認するなどを規定化する。
  3. 相手方の実在を対面で確認した以外のメールの送信者はなりすましである可能性が否定できないため、対面もしくは相手方代表電話を経由し実在の確認ができた相手方に限り、リンク、添付文書の閲覧を実施する。

### 攻撃の手口

* 1. マルウェアの初期侵入は、メールに添付した悪意ある文書ファイルや、悪意あるサイトへ誘導する埋め込みされたリンクである。OSやアプリケーションの脆弱性を利用し、Webサイトを閲覧しただけで、マルウェアが送り込まれる。マルウェアはブラウザーのID/Passwordを窃取し、システムへの攻撃や水平展開に利用する。

### 現状の課題

* 1. 攻撃者はユーザーとメールのやり取りを数回し、信頼を得たところで、悪意ある文書やリンクを送付してくる。信頼関係があるため、ファイルやリンクを開き被害にあってしまう。

### 対策の効果

* 1. 不審なサイトの閲覧を極力回避することで、被害を軽減できる。特に HTTPS で始まらない、鍵マークが表示されないサイトへの接続を禁止する規程を整備し、周知する。

### リスク受容

* 1. Google Chrome は既に HTTPSでなくHTTPのみ で始まるサイトへの接続に警告を発している。2020年10月からは HTTPのみ で始まるサイトからのダウンロードをブロックする予定である。今後、 HTTPS で始まらない、つまりドメインや組織の存在が確認できないサイトの閲覧は、脅威であると認識すべきであり、リスク受容は推奨できない。

### 対策による弊害の緩和

* 1. Chrome を使用する場合は、安全と考えられる HTTPのみ で始まるサイトを登録することで、ブロックを回避できる。

### 参考5.8 多要素認証機能の利用

### 設定・運用対策

* 1. 多要素認証を利用する。
  2. システム管理者の場合、多要素認証は必須とする。

### 攻撃の手口

* 1. 侵入したマルウェアは、ブラウザーやOSが保存しているID /PWなどの情報を窃取し、特権昇格や他の端末への水平展開を試みる。

### 現状の課題

* 1. パスワードは知識（記憶）に頼った認証方式である。一般的に、複雑で長い桁数のパスワードは記憶が困難なため、パスワードを使いまわすか、多少、変更して使いまわすことが多い。このため、何らかの方法でパスワードが漏洩すると、類似のパスワードを生成され、Webサイトやドメインに侵入されてしまう可能性が高い。また、パスワードの場合、漏洩したこと自体を検知するのが困難なため、定期変更が求められるが、定期変更までに攻撃が完了しているかもしれず、

### 対策の効果

* 1. 多要素認証は、知識もしくは生体情報と、所有（ハードウェア）の組み合わせて認証を行うもので、万一、パスワードもしくは生体情報が漏洩しても、所有物がなければ認証が成功しない。所有物を紛失、盗難して、パスワードが試行されても、パスワードのロックアウトが実施され、ブルートフォース攻撃は成功しない。

### リスク受容

* 1. 多要素認証は導入にコストがかかることがあり、移行期間、既存のシステムの認証方式との整合性が取れない場合がある。多要素認証を導入しない場合、ブルートフォース攻撃、辞書攻撃の耐性が強いとされる、長い桁数のパスフレーズの導入を行い、リスクを受容することが考えられる。
  2. システム管理者のリスク受容は推奨できない。

### 参考5.9 セキュアなネットワークの利用

### 設定・運用対策

* 1. Free Wi-Fi は利用禁止とし、携帯電話でのテザリングを利用する。
  2. 例外的にセキュアでないネットワークに接続する際は、組織もしくは信頼できるプロバイダーまで VPN 接続を行う。

### 攻撃の手口

* 1. 攻撃者は通信が暗号化されない Free Wi-Fi などで通信を傍受し、認証情報の窃取、システムへの侵入を試みる。特に、認証情報が暗号化されずに送信された場合、なりすましを許してしまう。また、実在する正規のAPと同一のSSID、暗号化キーを設置し、Free Wi-Fiのなりすましを行い、通信を傍受するなどが実例として存在する。
  2. 退職者が組織の Wi-Fi の事前共有鍵 (PSK) を利用し、若しくは第三者に暴露し、構外から Wi-Fi に接続する可能性がある。

### 現状の課題

* 1. 総務省の調査では、65%がFree Wi-Fi の危険性を認知していながらも、48%が実際にはなんら対策を施していないという調査がある。
  2. 退職者が出た場合に Wi-Fi の PSK を変更する組織は少なく、情報漏洩・窃取の脅威が存在している。

### 対策の効果

* 1. テザリングを利用し Free Wi-Fi に接続しないことで、情報窃取・漏洩のリスクを緩和できる。
  2. ゲストエリアでの組織内 Wi-Fi の AP を設置しない、月次で Wi-Fi の PSK を変更することで、退職者が出ても、情報窃取・漏洩のリスクを緩和できる。
     1. それぞれ、実効性を担保するため、規程を整備することが望ましい。

### リスク受容

* 1. セキュアでないネットワークの利用は、情報窃取・漏洩のリスクが高く危険で、リスク受容は推奨できない。

### 対策による弊害の緩和

* 1. やむを得ずセキュアでないネットワークを利用する際は、VPNソフトウェアを利用し、組織もしくは信頼できるプロバイダーまで、VPN で接続し、セキュアでないネットワーク内での暗号化通信を実施する。

### 参考5.10 外部記憶媒体の利用制限

### 設定・運用対策

* 1. USBメモリ等のリムーバブルメディアの利用を、職務上、やむを得ない場合を除いて許可しない。
  2. リムーバブルメディアを接続する端末は、自動再生を許可しない、自動実行コマンドの実行しない設定を行う。
  3. 可能な限り、リムーバブルメディアはアンチウイルス内蔵のものに限定する。
  4. 使用が終わったら初期化する。

### 攻撃の手口

* 1. マルウェアは常時、リムーバブルメディアの接続を監視しており、接続された段階で、リムーバブルメディアに自分自身をコピーし、自動再生機能、自動実行機能を悪用し他の端末への拡散を行う。

### 現状の課題

* 1. 客先等で、大量のデータを交換する際に、電子メールや Web アプリケーションを経由することが阻まれるケースがあり、やむなく、リムーバブルメディアを利用せざるを得ない状況が存在する。

### 対策の効果

* 1. 利用制限の内、リムーバブルメディアの接続の際の自動再生を禁止し、かつ、アンチウイルスソフト内蔵のリムーバブルメディアを利用することで、リスクを大幅に緩和することが可能である。

### リスク受容

* 1. 自動再生、自動実行の禁止は設定容易であり、再生もワンクリックするだけである。自動再生、自動実行のリスクがはるかに高く、受容すべきではない。

### 参考5.11 適切に管理・設定されたパスワードの利用

### 設定・運用対策

* 1. 初期パスワードは必ず変更する。
  2. ロックアウト可能なシステムの場合は、10回連続して間違ったら15分間、ロックアウトを実施する。
  3. 長いパスフレーズを採用する。

### 攻撃の手口

* 1. ルーター、Firewall、IoT 機器の変更されていない初期パスワードは、Web上で多数公開されている。攻撃者は、ブルートフォースや辞書攻撃でインターネットの接続点を攻撃してくる。また、電子メールやWebサイト経由で侵入したマルウェアは、水平展開を行う際に、それまで収集したID、パスワードをもとに推測したパスワードで侵入を試みる。
  2. IoT 機器や Windows の Built-in Administrator の場合、パスワード試行失敗のアカウントロックアウトができないため、ブルートフォースや辞書攻撃は極めて有効である。

### 現状の課題

* 1. ロックアウトが設定された場合、パスワードは8桁、英大文字、英小文字、記号の組み合わせで十分といえるが、上述のようにロックアウトができないシステムの場合、例えば”Ipa#9801” という英数字（大文字、小文字を含む）と記号を使った8桁のパスワードでも一般的な家庭用コンピュータを使って、12日で解読可能[[15]](#footnote-15)となる。

### 対策の効果

* 1. ”Ipa ha komagome” (長さ20桁）のような長いパスフレーズの場合、2896世紀かかるとされている。複雑性を要求するよりも、覚えやすいパスフレーズで長さを要求したほうが安全である。

### リスクの受容

* 1. システムの都合上、長い桁数を受け入れない、かつ、ロックアウトができないシステムが存在する。その場合は、極力、複雑かつ完全にランダムで可能な限り長いパスワードを設定する。総当たり攻撃がないか、定期的に監査を行い、兆候がある場合は、パスワードの有効期間を短く設定し、変更するなどを規程化して受容する。システム更新を早め、長い桁数を受け入れる、もしくは、ロックアウト可能なシステムに入れ替える。

### 対策による弊害の緩和

* 1. 辞書に掲載されていない単語を採用することが望ましいが、完全にランダムなパスワードは入力間違えも多く発生する。管理者端末からリモート接続の場合に限ってのみ、管理者のパスフレーズで暗号化保存したパスワードファイルからのコピー & ペーストを許可する。

## 【参考6： デフォルト緩和策　セキュリティ仕様・Webアプリケーション編】

### 参考6.1 暗号化

#### ・アプリケーションは、暗号で保護されたパスワードのみを送信すること。

パスワードを送信するときにパスワードを暗号化するようにアプリケーションを構成する。

#### ・アプリケーションは、送信される情報の機密性と整合性を保護すること。

データ保護要件に従ってTLS暗号化を要求するように、すべてのアプリケーションシステムを構成する。

### 参考6.2 脆弱性管理

#### ・アプリケーションは、オーバーフロー攻撃に対して脆弱であってはいけない。

自動境界チェックを実行する言語またはコンパイラを使用するようにアプリケーションを設計する。

抽象化ライブラリを使用して、危険なAPIを抽象化する。

StackGuard、ProPolice、Microsoft Visual Studio / GSフラグなどのコンパイラベースのカナリアメカニズムを使用する。

OSレベルの保護機能を使用し、ユーザー入力の検証を制御する。

ベンダー製品でオーバーフローが特定された場合、アプリケーションにパッチを適用する。

#### ・システムの初期化が失敗した場合、シャットダウンが失敗した場合、またはアプリケーション中止処理が失敗した場合、アプリケーションは安全な状態に失敗させる。

初期化、シャットダウン、中止などで、アプリケーションが安全でない状態があった場合、その脆弱性を修正する。

#### ・アプリケーションは、入力処理の脆弱性の影響を受けない。

ユーザー入力を受け入れるときはベストプラクティスに従い、アプリケーションが入力を処理する前にすべての入力が検証されることを確認する。特定された脆弱性を修正し、すぐに修正できない問題について文書化されたリスク許容度を取得する。

#### ・すべての製品は、ベンダーまたは開発チームによってサポートされること。

アプリケーション内のサポートされていないすべてのソフトウェア製品を削除または使用停止にする。

#### ・メンテナンスまたはサポートが利用できなくなったら、アプリケーションを廃止する。

アプリケーションのメンテナンスが継続されていることを確認する。

#### ・アプリケーションは、XML指向の攻撃に対して脆弱であってはならない。

XML攻撃に対して脆弱ではないコンポーネントを利用するようにアプリケーションを設計する。

脆弱性が発見されたら、アプリケーションコンポーネントにパッチを適用する。

#### ・アプリケーションは、SQLインジェクションに対して脆弱であってはならない。

アプリケーションを変更し、SQLインジェクションの脆弱性を削除する。

#### ・アプリケーションは、コマンドインジェクションから保護する。

特殊文字入力をエスケープ/サニタイズするようにアプリケーションを変更するか、アプリケーションアーキテクチャに基づいてコマンドインジェクション攻撃から保護するようにシステムを構成する。

#### ・アプリケーションは、クロスサイトスクリプティング（XSS）脆弱性から保護する。

ユーザー入力が検証されていることを確認し、ユーザー入力をエンコードまたはエスケープして、埋め込みスクリプトコードが実行されないようにする。

独自のエスケープロジックを構築するのではなく、Webテンプレートシステムまたは自動エスケープ機能を提供するWebアプリケーション開発フレームワークを使用して、アプリケーションを開発する。

### 参考6.3 セッション管理

#### ・アプリケーションは、ログオフ時またはブラウザーのクローズ時にセッションID値やCookieを破棄する。

アプリケーションセッションが終了したら、セッションID Cookieを破棄するようにアプリケーションを構成する。

#### ・アプリケーションはセッションIDを公開しない。

セッションIDを傍受または改ざんから保護するようにTLS、VPN等でアプリケーションを構成する。

#### ・アプリケーションは、非表示フィールドに機密情報を保存しない。

非表示フィールドに機密情報を保存しないようにアプリケーションを設計および構成する。ユーザーセッション管理にサーバー側セッション管理技術を使用する。

### 参考6.4 属性管理

#### ・アプリケーションには、必要に応じて機密属性を表示する機能が必要。

アプリケーションは、データの機密属性（個人情報、機微情報等）を、画面や印刷物に適切に表示する。

### 参考6.5 認証・認可

#### ・アプリケーションは、ユーザーによる15分間の無効なログオン試行を3回連続して制限する。

15分間に3回ログオンに失敗すると、アカウントロックを強制するようにアプリケーションを構成する。

#### ・アプリケーションに埋め込み認証データを含めることはできない。

コード、構成ファイル、スクリプト、HTMLファイル、またはASCIIファイルに認証データを埋め込まない。

#### ・SAMLアサーションでSubjectConfirmation要素を使用する場合、アプリケーションはNotOnOrAfter条件を使用する。

SAMLアサーションで<SubjectConfirmation>要素を使用するときに、<NotOnOrAfter>条件を使用するようにアプリケーションを設計および構成する。

#### ・WS-SecurityまたはSAMLアサーションを使用して、すべてのアプリケーションメッセージで有効期間を検証する。

すべてのWS-SecurityトークンプロファイルおよびSAMLアサーションで有効期間が検証されるようにする。

#### ・SAMLアサーションでConditionsエレメントを使用する場合、アプリケーションはNotBeforeエレメントとNotOnOrAfterエレメントの両方、またはOneTimeUseエレメントを使用する。

SAMLアサーションで<Conditions>要素を使用するときに、<NotBefore>および<NotOnOrAfter>または<OneTimeUse>の使用を実装するようにアプリケーションを設計および構成する。

#### ・WS-Securityで保護されたメッセージは、作成および有効期限付きのタイムスタンプを使用する。

WS-Securityメッセージを使用してアプリケーションを設計および構成し、作成および有効期限のタイムスタンプとシーケンス番号を使用する。

#### ・アプリケーションは、PKIベースの認証を使用する場合、対応する秘密キーへの承認されたアクセスを強制する。

アプリケーションまたは関連するアクセス制御メカニズムを構成して、アプリケーション秘密鍵への許可されたアクセスを強制する。

#### ・アプリケーションは、パスワード/ PINをクリアテキストとして表示しない。

入力時にパスワードとPINが難読化され、読み取れないようにアプリケーションを構成する。

難読化されたパスワードをコピーしてクリアテキストとして貼り付けることができないように、アプリケーションを設計する。

#### ・アプリケーションは、PKIベースの認証を利用する場合、受け入れられたトラストアンカーへの証明書パス（ステータス情報を含む）を構築することにより証明書を検証する。

PKIベースの認証を使用する場合、受け入れられたトラストアンカーへの証明書パスを構築するようにアプリケーションを設計する。

#### ・アプリケーションは、15文字以上のパスワード長を強制する。

パスワードに15文字を要求するようにアプリケーションを構成する。

#### ・アプリケーションは、過度のアカウント権限なしで実行する。

最小限の特権でアプリケーションアカウントを構成してください。アプリケーションが管理者資格情報で動作することを許可しない。

#### ・デフォルトのパスワードを変更する。

可能な場合、パスワードの代わりに強力な認証システムを使用するようにアプリケーションを構成する。そうでない場合は、デフォルトのパスワードを承認済みの強度のパスワードに変更し、パスワードに関するすべてのガイダンスに従う。

#### ・アプリケーションは、アクセス制御ポリシーに従って、情報およびシステムリソースへの論理アクセスに対して承認を実施する。

アプリケーションリソースへのアクセス承認を強制する。

#### ・アプリケーションは、組織ユーザー（または組織ユーザーに代わって動作するプロセス）を一意に識別して認証する。

ユーザーおよびユーザープロセスを一意に識別および認証するようにアプリケーションを構成する。

#### ・アプリケーションは、パスワードの暗号表現のみを保存する。

パスワードハッシュ値を作成するときは、強力な暗号化ハッシュ関数を使用する。

パスワードハッシュの作成時にランダムなソルト値を使用する。

認証データを含むデータファイルの強力なアクセス制御許可を確認する。

### 参考6.6 ネットワーク構成

#### ・アプリケーションWebサーバーは、DMZで動作する階層型アプリケーションである場合、アプリケーションサーバーおよびデータベースサーバーとは別のネットワークセグメントに存在する必要がある。

他のアプリケーション層からWebサーバーを分離し、DMZデータアクセス制御要件に従って、アプリケーションサーバーおよびデータベースサーバーとは別のネットワークセグメントに配置する。

## 【参考7：汚染される開発環境】

**広がるオープンソースの活用**

近年、ITシステムだけではなくIoTの分野でもオープンソースソフトウェア（OSS）の採用が広がっている。OSSの採用範囲がOSをはじめ、ミドルウェア、ライブラリ、コンポーネントから開発環境そのものまで多岐にわたる状況にある一方で、OSSに内在する「脆弱性」「ライセンス問題」について認知が進んできており、近年「正規の手段」でOSSに悪意のあるコードが仕込まれ、ユーザーに配布されるケースが発生している。

**オープンソースプラグインによる開発環境汚染事例**

ECD（Eclipse Class Decompiler）はJavaシステム開発で利用される、オープンソースの統合開発環境（IDE）である。プラグインシステムを採用しており、エディタやさまざまな機能をプラグインにより拡張することができる。例として、コード入力支援、リファクタリング支援、オンラインでバッグ、バージョン管理システムとの統合、Junitとの統合など開発効率化のための機能があり、デファクト的なIDEとして知られているが、これにはマルウェアが混入していることが明らかとなり、Eclipse Foundationの判断によりマーケットプレイスから強制的に削除された。このマルウェアは開発環境情報をローカルのJSONファイルに保存し、任意のサーバーに自動的に送信されていたことが確認されている。

この事件の問題は、公式サイトで配布されたバイナリが、リポジトリで公開されているソースと異なるところにある。人気プラグインであるEclipse Class Decompiler がEclipse公式マーケットで配布され、日本語標準Eclipseパッケージ（Pleiades All in One）にも採用されたものであり、業界に大きな影響を与えた。

**その他のバックドア関連の不正コードを含むコンポーネント**

インターネット上に公開されているバックドア関連の不正コードを含むコンポーネントを検索すると、以下のようにヒットする。今後も開発環境を狙った不正コードを含むコンポーネントは増加傾向にあり、システム開発受託業務に関連する企業は、FOSSの脆弱性管理の重要性を認識するべきである。



参考＿図 　バックドア関連の不正コードを含むコンポーネントの例

## 【参考8：セキュアコーディングガイド】





1. 一般的ユーザーのセキュリティ技術レベルを鑑み、「図1：セキュリティ仕様検討プロセスのイメージ」では企画支援プロセスでRFP提示を示しているが、一部の技術レベルの高いユーザーにおいては外部設計作成プロセスにおいてユーザー側からセキュリティ仕様をRFPに記述し、それを実装可能とするベンダーを選定することが想定される。これはシステム開発業務全体の効率や見積精度、リスク管理などの観点から理想的であるため、本章において2通りの解説をしている。 [↑](#footnote-ref-1)
2. 原因調査（外部攻撃、内部犯、オペレーションミスもしくはシステム不具合か？等の原因の特定）は想定以上に時間を要するか究明できないことが多い。 [↑](#footnote-ref-2)
3. 平均的なセキュリティ対策を講じているという趣旨の弁明は、社会的責任やステークホルダーへの影響が大きい組織におけるインシデントにおいてあまり意味をなさない。セキュリティ対策が平均以上でも事業継続に大きな影響を及ぼすことは、これまでの事例から明らかである。 [↑](#footnote-ref-3)
4. JPCERT/CC JVNDB RSS Feed 2019年1月4日－12月27日の件数 [↑](#footnote-ref-4)
5. MITRE ATT&CK 2019年9月時点で 324件 [↑](#footnote-ref-5)
6. MITRE は米国の非営利法人として、防衛、航空、国土安全保障、裁判所、健康、サイバーセキュリティの研究や公益に取り組無組織。米国国立標準技術研究所（NIST）の国立サイバーセキュリティFFRDC（NCF）の運営を行い、官民パートナーシップおよびハブとしての機能を提供。また、国土安全保障省の資金を得て、世界中の脆弱性情報に対して採番を行うCVE（Common Vulnerabilities and Exposures） の運用を行う。ATT&CK はこのCVEをもとに、脆弱性を悪用した実際の攻撃を戦術単位で分類したナレッジベースである。 [↑](#footnote-ref-6)
7. ここで採用されている対策・緩和策は、OSや管理サーバーでの設定によるものである。一般的にOSは広く接続する方向で出荷時設定がなされているが、情報セキュリティ維持のために接続を制限する設定を行うことも可能である。また、デスクトップアプリケーションやブラウザーも出荷時設定以外のセキュリティ強化設定が可能となっており、セキュリティガイドラインはこのような設定を多く採用している。 [↑](#footnote-ref-7)
8. 民間のサイバー救急対応サービス等で確認される実際に発生した脅威情報と、ペネトレーションテスターの見識による攻撃のしやすさを各3段階に評価し、双方が最高値(3)であったものを対策すべき重要脅威としている。これにより、低コストで実践的な防御対策を講じ、攻撃ベクトルの中での効果的な封じ込めを目指した。 [↑](#footnote-ref-8)
9. 米国国防総省 Security Technical Implementation Guides (STIGs) は、製品の安全な展開の実装を支援するように設計されたガイドライン。2020年3月時点で、402製品/ポリシーガイド/ツール（ドラフトを含む）が掲載されており、Network機器、セキュリティ製品、OS、アプリケーションソフト、データベースがバージョン毎に公開されている。さまざまなベンダーやコミュニティからの提案を受け、逐次、改訂されている。多くのサードパーティがSTIG Viewerを提供しており、各製品の設定データをXML、JSON、CSVで入手できる。 [↑](#footnote-ref-9)
10. 当該システムだけでなく、全社機能として日頃より自社が受ける法的な規制やガイドラインを明確化し、各システムが規制対象となる場合の法令等と遵守事項、罰則などを文書化しておく。特に個人情報保護法は3年毎の見直しに連携し、業界向けのガイドラインの改定もあるため留意する。また、GDPRを始めとする他国の規制について、関連があれば文書化しておく。 [↑](#footnote-ref-10)
11. バージョンの限定、IT情報資産およびネットワーク仕様の明示ならびに第三者ソフトウェア等に関する事項 [↑](#footnote-ref-11)
12. 働き方改革で、在宅勤務や社外サテライトから企業ネットワークに接続する機会が増加傾向にあるため、社外ネットワークに接続されるノートPCやスマートフォンのセキュリティ維持は必要。在宅勤務で使用するPCと家庭内ネットワークの健全性も同様。企業ネットワークに脆弱性がなくとも、在宅時に接続するルーターやPCに脆弱性があれば重大な脅威となる。 [↑](#footnote-ref-12)
13. デフォルト緩和策の前提条件として、サポート切れソフトウェア（OS・アプリケーション）は使用していないことを前提とする。利用者はサポート内（できる限り最新のバージョンの）製品を利用し、最新のパッチが適用されたソフトウェアを利用するとともに、ソフトウェアの推奨指定されている機能については出来る限り利用する。 [↑](#footnote-ref-13)
14. FOSS以外のコンポーネントは、脆弱性の発生時やEoLの際の対応に関する記述、および有償保守、無償対応等の明記が必要とされるが、FOSSの採用責任に関しては外部設計書もしくはセキュリティ仕様書に明示する。「モデル取引・契約書」の49条には、「3. 乙は、FOSSに関して、著作権その他の権利の侵害がないこと、及び契約不適合のないことを保証するものではなく、乙は、第一項所定のFOSS利用の提案時に権利侵害又は契約不適合の存在を知りながら、若しくは重大な過失により告げなかった場合を除き、何ら責任を負わないものとする。」とあり、FOSSは権利侵害や契約不適合（不具合等）がないことを保証するものではないことを前提に採用するため、外部設計の時点で、権利侵害や契約不適合（不具合等）があることを知っていた、若しくは、ベンダーの重大な過失により告知しなかったこと以外は責任を取らないとする。 [↑](#footnote-ref-14)
15. https://password.kaspersky.com/jp/ [↑](#footnote-ref-15)