サイバーセキュリティフレームワークを応用したアセスメント

Assessment by Applying Cyber Security Framework

福　田　俊　介

要　約　日本ユニシスは，組織のセキュリティ対策の成熟度やリスクを計測して今後の対応の方向性を定め，経営層と共有して継続的なサイバーセキュリティ経営の実践に寄与するためのアセスメントを実施している．アセスメントには米国国立標準技術研究所（NIST）が公開したサイバーセキュリティフレームワーク（CSF）を用いる．CSF はコア，インプリメンテーションティア，プロファイルの三つのコンポーネントから成り，アセスメントでは前 2 者を用いる．アセスメントは準備，現状把握，評価，報告，実行計画の 5 ステップで実施する．準備段階でのアセスメントシートの設計は慎重に当たらなければならず，また結果の関連部署や経営層への報告，共有も極めて重要なプロセスである．サイバーセキュリティにおけるアセスメントはあくまでもリスクを評価し実行計画を策定するための作業であり，リスク対応活動を確実に実行し，リスク低減に寄与することがアセスメント実施の最終目的である．

Abstract　The assessment conducted by Nihon Unisys is to measure the maturity and risk of security measures of the organization, and also to determine the future directionality, This assessment is carried out to contribute to the practice of continuous cyber security management. The assessment uses the Cyber Security Framework (CSF) published by the National Institute of Standards and Technology (NIST). The CSF consists of three components: core, implementation tier, and profile, and the first two are used in the assessment. Assessment is carried out in 5 steps. Namely, preparation, current situation, evaluation, report, and action plan. The design of the assessment sheet at the preparation stage must be carefully applied, and the reporting and sharing of the results to relevant departments and management is also an extremely important process. The assessment in cyber security is the task to evaluate the risk and formulate an action plan, and it is the final purpose of the assessment to carry out the risk response activities and contribute to the risk reduction.

1. は　じ　め　に

サイバーセキュリティとは，インターネットを中心とするサイバー空間における安全を確保するための包括的な概念として ISO/IEC 27032:2012（Information technology — Security techniques — Guidelines for cybersecurity）で「サイバー空間において機密性，完全性，可用性の確保を目指すもの」と定義されている．情報資産に対する機密性，完全性，可用性を確保する概念は，従来の情報セキュリティの基本的な考え方と同様であるが，サイバー空間における脅威に対するセキュリティを取り扱う点において特異性がある．今やインターネットに接続されない組織は存在しないと言っても過言ではない時代におけるサイバーセキュリティの確保は，全組織共通の経営課題となった．従来から情報セキュリティの確保に経営資源を投入してきた組織でもサイバーセキュリティへの対応に適合することは容易ではない．サイバー空間

における脅威や脆弱性が常に変化すること，サイバーセキュリティのリスクを低減するための対策技術の進展が早く，それらを迅速にキャッチアップすることが難しいこと，セキュリティ対策の投資対効果が不透明であるため計画的な投資に困難を伴うこと，サイバーセキュリティに対応するための専門人材の確保や育成が困難であること，等がその要因として挙げられる．サイバーセキュリティへの対応は一過性であってはならず，経営層が直接関与する戦略および一貫性のある枠組みに基づき，リスクベースアプローチによる継続的な取り組みでなければならない．

本稿では，サイバーセキュリティの包括的フレームワークを用いて日本ユニシス株式会社が実施したアセスメントを基に「サイバーセキュリティアセスメント」について提言する．サイバーセキュリティアセスメントの目的は，従来の情報セキュリティの枠組みをサイバーセキュリティに適合させるため，包括的なサイバーセキュリティのフレームワークに基づき自組織の現状を可視化し，セキュリティ対策の成熟度やリスクを計測して今後の対応の方向性を定め，経営層とも共有することで継続的なサイバーセキュリティ経営の実践に寄与することである．2章にてアセスメントで使用したサイバーセキュリティフレームワークについて，3章でアセスメントの実施プロセスと手法について述べ，4章にてアセスメントで導出した対応の施策化等をまとめた．本稿での紹介を通して，他組織におけるサイバーセキュリティ推進の一助になれば幸いである．

2. サイバーセキュリティフレームワーク

セキュリティアセスメントとは，組織におけるセキュリティ対策状況を把握することで，セキュリティに関わるリスクを可視化し，今後の対応を定めるための一連の活動を指す．自組織が準拠すべき特定のセキュリティ基準やベストプラクティスを使用した広範囲なベースライン型アプローチと，特定の情報システム等の比較的狭い領域を対象とした詳細分析型アプローチの二種が存在し，前者は組織全体におけるセキュリティリスクを，後者は組織における重要な情報システムやサービスにおけるセキュリティリスクをコントロールするために使い分け，あるいは併用される．本稿で紹介するセキュリティアセスメントは，組織全体に関わるサイバーセキュリティを網羅的に点検するので，前者のベースライン型アプローチに該当する．

セキュリティアセスメントで採用したベースラインは，米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が2014年2月に初版を公開したサイバーセキュリティフレームワーク（Cyber Security Framework：CSF）の最新バージョン（第1.1版：2018年4月公開）である[1][2]．CSFは，主に重要インフラ事業者を対象とした国際的に権威あるフレームワークであり，従来の情報セキュリティ国際標準であるISMS（Information Security Management System，ISO/IEC 27001/27002），COBIT（Control Objectives for Information and Related Technology），およびCIS（The Center for Internet Security）が発行するサイバーセキュリティ防御に有効な対策について論じたガイドラインであるCSC（The CIS Critical Security Controls for Effective Cyber Defense）[3]等との整合が図られている．CSFは，昨今日本国内においても，重要インフラ事業者を中心に活用が推進されつつあり，サイバーセキュリティにおけるデファクトスタンダードと位置付けられるフレームワークである．

CSFは，フレームワークコア，フレームワークインプリメンテーションティア，フレームワークプロファイルの三つのコンポーネントにより構成される．本章の各節で説明する．

2.1　CSF フレームワークコア

CSF フレームワークコアは，サイバーセキュリティ対策のベストプラクティス集であり，識別（IDentify）」，「防御（PRotect）」，「検知（DEtect）」，「対応（ReSpond）」，「復旧（ReCover）」の五つの機能領域により構成されている．各機能領域は，機能配下に定義されるカテゴリ（23種）とその配下であるサブカテゴリ（108 種）の階層により構造化され，サブカテゴリについては実装面での参考とされる既存のセキュリティ標準やガイドラインにおける関連項目との対応付けがなされている．CSF フレームワークコアにおける機能とカテゴリを表 1 に示す．カテゴリ配下に定義されるサブカテゴリ等の CSF フレームワークコアの詳細については，参考文献[1]および[2]を参照いただきたい．

表 1　CSF フレームワークコアの基本構成

機能（略称）	カテゴリ	機能（略称）	カテゴリ
識別（ID）	資産管理	検知（DE）	異常とイベント
	ビジネス環境		継続的モニタリング
	ガバナンス		検知プロセス
	リスクアセスメント	対応（RS）	対応計画
	リスクマネジメント戦略		コミュニケーション
	サプライチェーン		分析
防御（PR）	アクセス制御		低減
	意識向上・トレーニング		改善
	データセキュリティ	復旧（RC）	復旧計画
	情報保護のプロセス手順		改善
	保守		コミュニケーション
	保護技術		

識別（ID）では，セキュリティ対策の対象となる資産，セキュリティポリシーに代表されるセキュリティガバナンス，リスクマネジメントといったサイバーセキュリティ戦略全体に関わる領域を，防御（PR）では，アクセス制御，セキュリティ教育や訓練，情報システム，ネットワーク，データ保護に代表される事前対策に関わる領域を，検知（DE）では，組織における SOC（Security Operation Center）に代表されるセキュリティイベントを迅速に検出するための仕組みやプロセスに関わる領域を，対応（RS）と復旧（RC）では，主に CSIRT（Computer Security Incident Response Team）に代表されるセキュリティインシデントの対応と復旧といった事後対策に関わる領域を扱う．従来の情報セキュリティ対策が，事前対策の領域に偏重していた状況を踏まえ，また「サイバーセキュリティインシデントを 100％防止することは困難」という事故発生前提の考え方に基づき，事前，事後のサイバーセキュリティ対策全体のバランスが考慮された構成となっていることが従来のセキュリティフレームワークと最も異なる点である．一般的に，事前対策に位置付けられる識別（ID）と防御（PR）の機能は，従来の情報セキュリティ対策として実施されてきた領域であるが，検知（DE），対応（RS），復旧（RC）といった機能は，より高い専門性が求められ対応難易度が高いサイバーセキュリ

ティ固有の領域と言える．フレームワークコアのベストプラクティスをベースラインとしたアセスメントを実施することにより，サイバーセキュリティの多様な機能，対策の網羅性を確認した上で，自組織で備えるべきサイバーセキュリティ能力を検討することが可能となる．

2.2　CSF フレームワークインプリメンテーションティア

CSF におけるフレームワークインプリメンテーションティアは，前節のフレームワークコアのベストプラクティスが対象組織においてどのレベルで実装されているかの達成度，成熟度を示す指標であると共に，組織におけるサイバーセキュリティ向上の目標値を設定するためにも使用される．フレームワークインプリメンテーションティアの定義と解釈を表 2 に示す．

表 2　CSF フレームワークインプリメンテーションティア

ティア	定　義	解　　釈
ティア 1	部分的である （Partial）	・リスク対応が定められておらず，対応は場当たり的 ・リスク意識が低く，リスクマネジメントが不安定 ・自組織内や関連組織との連携，情報共有も不充分
ティア 2	リスク情報を活用している （Risk Informed）	・リスク対応は経営層に承認されているが，組織全体のセキュリティポリシーとしては未策定 ・サイバーセキュリティ戦略が組織全体に浸透していない
ティア 3	繰り返し適用可能である （Repeatable）	・リスク対応は承認され，ポリシーにも反映されている ・サイバーセキュリティ戦略の継続的アプローチが確立されており，必要なセキュリティ能力を保持している
ティア 4	適応している （Adaptive）	・リスク対応は変化する脅威や技術の変化に対応できる ・サイバーセキュリティ戦略が自組織の文化に浸透しており，自組織の環境に対するリスクに柔軟に対応できる

ティアを目標値として使用する場合，そのティアを目指すための施策は実施可能なものであり，リスク低減に寄与できるものでなければならない．いたずらに高いティアを目標に設定すると，セキュリティ対策や運用に伴う負荷が増加し，結果的にレベルアップが図られない結果を招く恐れがあるので，注意を要する．CSF ではティアを割り付ける対象や単位を規定していないが，フレームワークコアのカテゴリまたはサブカテゴリに対して設定することが一般的であろう．また，ティア設定の精度に関しては，フレームワークコアにおけるカテゴリやサブカテゴリの担当部署の判断に加えて，自組織のビジネス環境やサイバーセキュリティ活動の状況を深く理解したセキュリティ有識者の判断を加えることが有効である．

2.3　CSF フレームワークプロファイル

フレームワークプロファイルは，自組織におけるフレームワークコア（機能，カテゴリ，サブカテゴリ）から抽出された対応の集合体であり，フレームワークインプリメンテーションティアを使用した現状と目標を付与することで，組織におけるサイバーセキュリティのロードマップを示すためのものである．CSF ではフレームワークプロファイルの雛形は提供されていない．

3. サイバーセキュリティフレームワークを活用したアセスメント

本章では，アセスメントの目的と実施プロセス及びアセスメントシートの設計について述べ，フレームワークコアの5領域におけるアセスメント例を紹介する．

3.1 アセスメント実施の目的

サイバーセキュリティフレームワークを使用したアセスメント実施の目的は以下の通りであり，いずれも，継続性が求められるサイバーセキュリティリスク対応の戦略的側面において重要なテーマである．

・従来実施してきたサイバーセキュリティ対策全体に関する現状の可視化
・リスクの高い領域を抽出し今後の重点対応施策，中期的なロードマップの設定
・サイバーセキュリティ関連予算全体の安定確保に向けた基礎情報の収集
・サイバーセキュリティに関わる取締役，CIO（Chief Information Officer）/CISO（Chief Information Security Officer）等経営層への報告，および情報共有

また，アセスメントは，自組織のサイバーセキュリティ戦略における活動の一環として実施することで，従来実施してきたISMS等をベースとしたセキュリティ対策との差異や実施の位置付けをより一層明確化することができる．サイバーセキュリティフレームワークというサイバーセキュリティ領域に特化したフレームワークを採用することで，未知/既知の脅威を対象とした技術的対策やインシデント・レスポンス体制といった対応の総合点検に加え，ビジネスエコシステムの形成等自組織におけるビジネスの動向を踏まえ，昨今急速に拡大しているクラウドサービスの利活用やサプライチェーンに対するリスクマネジメントといった新たなリスク対応への考察の契機とする．

3.2 アセスメントの実施プロセス

サイバーセキュリティフレームワークを使用したアセスメントの実施プロセスは表3の通りである．

表3　アセスメントの実施プロセス

ステップ	工　程	内　　容
ステップ1	準備	・アセスメントで使用するフレームワークの詳細を理解する ・アセスメントで使用するツール（アセスメントシート等）を設計する
ステップ2	現状把握	・フレームワークコアの機能領域単位でスケジュールを定め，各対策項目の主管部署を交えたミーティング形式で現状把握を行う ・現状に対する課題と対応策の案を導出する
ステップ3	評価	・インプリメンテーションティアにより現状における成熟度評価を行う ・現状，成熟度を踏まえてリスクの大きさを評価する ・ステップ2で導出した課題とその対応策の優先度を設定する
ステップ4	報告	・関連部署の管理層を交えアセスメント内容をレビューする ・CISOのレビューと承認を受ける ・CISOの上位マネジメントである取締役への報告を行う
ステップ5	実行計画	・導出された対応策について，各主管部署と実行計画および予算措置を協議，調整する

実施期間は，アセスメント対象とする組織や情報システムの規模に大きく依存する．経験に根ざした目安は，ステップ1が約1カ月，ステップ2および3が約3カ月，ステップ4および5が1～2カ月程度である．特にステップ2，3および5には充分な期間を設け，各主管部署とのコミュニケーションに配慮し，アセスメント結果を確実に実行可能なリスク対応計画に落とし込まなければならない．CSFで規定されるサイバーセキュリティリスク対応の範囲は多岐にわたり，単一のセキュリティ部署だけが対応するものではなく，組織内におけるセキュリティ管理統制部門，情報システム部門，品質管理部門，人材育成部門，CSIRT等を担当するセキュリティ専門部署等が円滑なコミュニケーションを図ることが極めて重要である．また，アセスメントの実施結果について，CISOをはじめとした経営層，取締役クラスの理解を得ることで，サイバーセキュリティ経営の継続性が担保されることに繋がる．アセスメントを単なる一過性の活動ではなく，サイバーセキュリティに関する有効なコミュニケーションツールとしても活用する戦略的活動として捉え，実施することが重要なのである．

3.3　アセスメントシートの設計

アセスメントに使用するシートは，ステップ1（準備）において，慎重に設計しなければならない．アセスメントシートの項目等に考慮漏れがあると，後続のステップで大きな手戻りに直結する可能性が高いためである．今回紹介するアセスメントにおける評価の基点は，CSFに定義されているフレームワークコアの階層（機能，カテゴリ，サブカテゴリ）であり，サブカテゴリのレベルで108項目ある．サブカテゴリはサイバーセキュリティに求められる一般的な対策要件のベストプラクティスに過ぎず，自組織に当てはめた解釈，およびアセスメントに使用するためには，いくつかの項目を追加したアセスメントシートを設計し，使用しなければならない．アセスメントシートに追加する項目には，サブカテゴリ（セキュリティ対策要件）の対象となる自組織における情報資産（組織，業務システム，システム基盤，業務プロセス等）や主管部署，現在の対応状況や課題と対策（セキュリティソリューションの導入を含む）等の定性的な情報，成熟度やリスクの大きさ，リスク低減策の優先度等の数値的な情報が含まれる．数値的な情報については，過度な詳細化を行っても，複雑化するデメリットの方が大きいため，3～4段階程度の基準値を使用する．アセスメントシートに追加する主要な項目について表4に示す．

表4　アセスメントシートの追加項目

追加項目	説　　明
情報資産	CSFサブカテゴリの対策要件の適用対象となる自組織の情報資産 ・組織/要員（セキュリティ委員会，リスク管理体制，CSIRT，経営層，従業員，セキュリティ要員 等） ・業務システム（基幹システム，部門システム，社外公開サイト，利用している外部クラウドサービス 等） ・システム基盤（データセンター，社内ネットワーク，インターネット接続，PCやファイル共有サーバ等のOA基盤，プライベートクラウド，会社支給のスマートフォン，外部媒体 等） ・業務プロセス（リスク管理プロセス，システム開発プロセス，品質管理プロセス，外部委託プロセス，セキュリティ教育プログラム，事業継続計画 等）

主管部署	CSF サブカテゴリ×情報資産の組み合わせにおける対象領域のセキュリティを担当する主管部署 ・リスク/セキュリティ管理部門 ・情報システム部門（企画，管理，アプリケーション開発，システム基盤，システム運用） ・人事/法務/品質管理/人材育成部門 ・顧客サービス部門（営業，IT 部門 等） ・セキュリティ技術主管部門 等
現状と根拠	CSF サブカテゴリ×情報資産の組み合わせにおけるセキュリティの実施状況およびその根拠となる情報
課題と対策	CSF サブカテゴリ×情報資産の組み合わせにおけるセキュリティの課題およびその改善策の案 ・セキュリティポリシーや各種規程，手順書等の改善 ・システムおよびセキュリティ運用管理の改善 ・業務プロセスの改善 ・体制の見直し，人材の育成 ・セキュリティソリューション（製品/サービス）の導入 等
成熟度	CSF サブカテゴリにおけるセキュリティに対する CSF フレームワークインプリメンテーションティアに基づく，成熟度の指標（ティア 0 については CSF の定義には含まれないが，独自に追加する場合がある） ・ティア 0：全く実施していない ・ティア 1：部分的である（Partial） ・ティア 2：Risk 情報を活用している（Risk Informed） ・ティア 3：繰り返し適用可能である（Repeatable） ・ティア 4：適応している（Adaptive）
リスクの大きさ	CSF サブカテゴリ×情報資産の組み合わせにおける現状のセキュリティリスクの大きさを示す指標 ・レベル 1：リスクはほぼ無い，または極めて小さい ・レベル 2：リスクは中程度 ・レベル 3：リスクが大きい ・レベル 4：リスクが極めて大きい
対応優先度	CSF サブカテゴリ×情報資産の組み合わせにおける今後のリスク対応の優先度指標 ・優先度 低：リスク受容または長期的に検討（リスクレベル 1） ・優先度 中：中期的にリスク対応を検討（リスクレベル 2） ・優先度 高：緊急性が高いリスク対応（リスクレベル 3 以上）

特に留意すべき事項は，情報資産を細かく捉え過ぎないこと，主管部署が特定できない，あるいは複数組織に跨るケース（役割が曖昧）があり得ること，現状と根拠はできる限り正確に記すこと，指標の設定には有識者を介在させることなどである．尚，リスクの大きさとは連動しないが，対応優先度には対応の実施負荷を考慮し，短期間で容易に実施できると判断される追加対策の一部も優先度 高とする配慮を行う場合もある．

3. 4　アセスメントの例

CSF フレームワークコアにおける機能：識別（ID），防御（PR），検知（DE），対応（RS），復旧（RC）の各領域における代表的なアセスメントの例を示す．

3. 4. 1　識別（ID）

識別（ID）は，サイバーセキュリティフレームワークにおける上流領域であり，そのカテゴリは，アセットマネジメント（AM），ビジネス環境（BE），ガバナンス（GV），リスクアセスメント（RA），リスクマネジメント（RM），サプライチェーン（SC）といった内容で構成されている．組織においてサイバーセキュリティの全体統制に関わる管理部門が主管する機能が多く含まれている領域であり，各カテゴリの配下に位置するサブカテゴリ数は合計で 29 項目が存在する．サイバーセキュリティの対象となる情報資産やサプライチェーンを識別管理し，自組織のビジネス環境変化を踏まえ，リスク管理の視点で組織全体のセキュリティ統制を図ることが識別（ID）領域の目的である．従来から実施されてきた情報セキュリティポリシーの運用等もこの領域に属するものである．

識別（ID）におけるアセスメント例（ID.RA-2：脅威と脆弱性情報の入手）は表 5 の通りである．

表 5　アセスメント例（識別（ID.RA-2：脅威と脆弱性情報の入手））

カテゴリ： ID.RA	**リスクアセスメント**：企業は自組織の業務（ミッション，機能，イメージ，評判を含む），自組織の資産，個人に対するサイバーセキュリティリスクを把握している		
サブカテゴリ： ID.RA-2	情報共有フォーラム/ソースより，脅威と脆弱性に関する情報を入手している		
情報資産 （適用対象）	①脅威情報の入手プロセス	②脆弱性情報の入手プロセス（脆弱性情報ハンドリング[*1]）	③インシデント情報の入手プロセス
主管部署	・CSIRT ・SOC	CSIRT	セキュリティ主管部署
現状	公的な第三者機関よりセキュリティの脅威情報を入手している． 使用しているセキュリティ製品はベンダーの脅威インテリジェンス情報[*2] と連携している．	CSIRT の脆弱性対応プロセスに則り，日次で脆弱性情報を収集し組織内へ配信している．	複数の情報ソースを定め，重大なインシデント情報を収集しポータルサイトで組織内へ情報共有している．
主要な課題	セキュリティ製品は脅威インテリジェンス情報と連携しているが，一定の誤検知/過検知が発生する．	収集した脆弱性情報と情報システムの構成情報が充分に相関分析できていない．	情報共有に関して，セキュリティ関連部署以外の認知度が低い．
課題に対する対策	製品のアップデートおよび運用チューニングによる精度の向上	脆弱性情報とシステム構成情報をマッチングする機能の強化	認知度向上のための継続的な啓蒙活動の実施
成熟度評価	評価値：3（繰り返し適用可能である：Repeatable） ※各種セキュリティ情報は継続的に入手され，情報共有が図られている		
現状のリスク	評価値：2（セキュリティ運用負荷の増加）	評価値：3（脆弱性対応の抜け漏れや遅延）	評価値：1（セキュリティ意識の低下）
対応の優先度	評価値：優先度 中	評価値：優先度 高	評価値：優先度 低

上記の例では，ID.RA-2（脅威と脆弱性情報等の入手）に関して，②脆弱性情報ハンドリングにおける対応遅延リスクの低減を重要と捉え，改善策（脆弱性情報配信システムの改善）の優先度を高に設定している．

3. 4. 2　防御（PR）

防御（PR）は，サイバーセキュリティフレームワークにおけるセキュリティ対策（事前対策）の領域であり，そのカテゴリは，アクセス制御（AC），意識と訓練（AT），データセキュリティ（DS），情報保護のプロセスと手順（IP），メンテナンス（MA），保護技術（PT）といった内容で構成されている．組織において技術的セキュリティ対策の設計や実装に関わる情報システム部門やセキュリティ教育等の人材育成部門が主管する機能が多く含まれている領域であり，各カテゴリの配下に位置するサブカテゴリ数は合計で 39 項目が存在する．識別（ID）領域の統制に従い，サイバーセキュリティの技術的対策や教育により，組織が保有する重要な情報資産やデータを保護することが防御（PR）領域の目的である．従来から実施されてきた技術的対策やセキュリティ教育等はこの領域に属するものである．

防御（PR）におけるアセスメント例（PR.AT-1：全てのユーザに情報を周知し，トレーニングを実施）は表 6 の通りである．

表 6　アセスメント例（防御（PR.AT-1：全てのユーザに情報を周知し，トレーニングを実施））

カテゴリ： PR.AT	**意識と訓練**：自組織の職員およびパートナーに対して，関連するポリシー，手順，契約に基づいたサイバーセキュリティに関連する義務と責任を果たせるようにするために，サイバーセキュリティ意識向上教育と十分なトレーニングを実施している		
サブカテゴリ： PR.AT-1	全てのユーザに情報を周知し，トレーニングを実施している		
情報資産 （適用対象）	①全役職員	② IT 技術者（システムエンジニア）	③セキュリティ専門要員
主管部署	セキュリティ管理部門	人材育成部門	セキュリティ管理部門 人材育成部門
現状	全役職員向けに定期および非定期でのサイバーセキュリティ教育を実施している．	IT 技術者向けのセキュリティ教育プログラムを定期的に実施している（集合技術教育，CTF[*3] 等）．	CSIRT 等セキュリティ専門家向けの教育プログラムを実施している（サイバーセキュリティ演習[*4] 等）．
主要な課題	教育の形骸化を防ぐために継続的に工夫すること．	IT 技術者のセキュリティスキルを具体化，可視化すること．	トレーニングには相応のコストが発生するため，教育予算を継続的に確保すること．
課題に対する対策	経営層や新入社員等を視野に入れた教育コンテンツの拡充を図る．	セキュリティ技術のスキルマップの最新化を図り，スキル調査に反映する．	人材育成部門の育成計画と連携した予算の継続確保を図る．
成熟度評価	評価値：3（繰返し適用可能である：Repeatable） ※教育対象は網羅されており，実施の継続性も保たれている		

現状のリスク	評価値：2（教育が形骸化する）	評価値：3（対象者が多く時間を要する）	評価値：2（スキルや経験に格差が生じる）
対応の優先度	評価値：優先度 中	評価値：優先度 高	評価値：優先度 中

上記の例では，PR.AT-1（全てのユーザに情報を周知し，トレーニングを実施）に関して，多様な IT システムやサービス開発に関わる② IT 技術者のセキュリティスキル向上が重要と捉え，改善策（IT 技術者のセキュリティスキルの可視化等）の優先度を高に設定している．

防御（PR）における二つ目のアセスメント例（PR.DS-5：データ漏えいに対する保護対策の実施）は表 7 の通りである．

表 7　アセスメント例（防御（PR.DS-5：データ漏えいに対する保護対策の実施））

カテゴリ：PR.DS	**データセキュリティ**：情報と記録（データ）を，情報の機密性，完全性，可用性を保護するために定められた自組織のリスク戦略に従って管理している		
サブカテゴリ：PR.DS-5	データ漏えいに対する保護対策を実施している		
情報資産（適用対象）	①社内システム上のデータ	②モバイル PC に保管されるデータ	③外部記憶媒体に保管されるデータ
主管部署	情報システム部門	セキュリティ管理部門	セキュリティ管理部門
現状	データベースやファイル共有サービスに対するアクセス制御を実施している．	モバイル PC へのローカルデータの保存を原則禁止，ディスク暗号化等を実施している．	外部媒体の利用を原則禁止，データファイルへのアクセス制御等を実施している．
主要な課題	インターネットからの不正アクセスに対するデータ漏えい対策の強化．	PC 紛失対策およびインターネットからの不正アクセスに対するデータ漏えい対策の強化．	外部媒体の不必要な利用を制限していることで一定の効果があるが紛失のリスクは残る．
課題に対する対策	セキュアクラウドストレージの利用拡大，次世代エンドポイントセキュリティ製品[*5] の有効活用を図る．	次世代エンドポイントセキュリティ製品の有効活用を図る．	セキュリティ教育等でリスクと対策の継続的な周知徹底を図る．
成熟度評価	評価値：2（リスク情報を活用している：Risk Informed） ※一定の対策が適用されているが，リスクやインシデントの状況に応じた新たな技術的対策の継続検討を要する		
現状のリスク	評価値：3（標的型攻撃等によるデータ漏えい）	評価値：3（モバイル PC の紛失）	評価値：2（外部媒体の紛失）
対応の優先度	評価値：優先度 高	評価値：優先度 高	評価値：優先度 中

上記の例では，PR.DS-5（データ漏えいに対する保護対策の実施）に関して，①社内システムおよび②モバイル PC におけるデータ漏えいリスクの更なる低減を重要と捉え，改善策（データ漏えい対策ソリューションの強化検討等）の優先度を高に設定している．

3. 4. 3　検知（DE）

CSF における検知（DE）は，セキュリティ脅威やインシデントを迅速に検出するための領

域であり，そのカテゴリは，異常とイベント（AE），継続監視（CM），検出プロセス（DP）といった内容で構成されている．組織において実装されている技術的セキュリティ対策をベースに一般的に SOC（Security Operation Center）と呼ばれるセキュリティ監視部門が主管する機能が含まれている領域であり，各カテゴリの配下に位置するサブカテゴリ数は合計で 18 項目が存在する．防御（PR）領域で実装された技術的セキュリティ対策であるセキュリティソリューションやサーバ，クライアント等のエンドポイントが出力するアラート，セキュリティログ等の情報を収集分析し，インシデントやその予兆であるセキュリティ脅威を検出することや，システムの脆弱性を検査することなどが検知（DE）領域の目的である．フレームワークコアの中でもセキュリティの専門知識と経験を要する領域であり，組織が保有するセキュリティ能力により，セキュリティ専門ベンダーが提供するアウトソーシングサービスが活用されるケースも多い．セキュリティ脅威を検出するためには，防御（PR）で採用するセキュリティソリューションとの連携が必須である．

検知（DE）におけるアセスメント例（DE.CM-8：脆弱性スキャンの実施）は表 8 の通りである．

表 8　アセスメント例（検知（DE.CM-8：脆弱性スキャンの実施））

カテゴリ：DE.CM	**継続監視**：サイバーセキュリティイベントを検知し，保護対策の有効性を検証するために，情報システム資産をモニタリングしている		
サブカテゴリ：DE.CM-8	脆弱性スキャン[*6]を実施している		
情報資産（適用対象）	①インターネット公開サービス	②イントラネット上の社内サービス	③顧客に提供する IT サービス
主管部署	・広報部門 ・情報システム部門	・情報システム部門（基幹系サーバ） ・事業部門（部門サーバ）	・品質管理部門 ・事業部門
現状	セキュリティ主管部により継続的な脆弱性スキャンおよび是正勧告を実施している．	継続的な脆弱性スキャンは実施していないが，セキュリティパッチが厳格に適用されている．	自社のシステムサービス開発標準の品質管理プロセスにおいて，脆弱性スキャンを実施している．
主要な課題	中小規模サイトのオーナにおけるコスト負担が生じている．	パッチ適用等の脆弱性対応が実施されており，大きな課題は見受けられない．	サービス運用開始後の継続的診断コストの軽減．
課題に対する対策	パートナー企業への一括委託および実施サイクルの見直しを図る．	特になし．	DevSecOps[*7]の整備，クラウド型脆弱性スキャンサービスの適用を検討する．
成熟度評価	評価値：3（繰り返し適用可能である：Repeatable） ※インターネットサービスに対する脆弱性診断が継続的に実施されている		
現状のリスク	評価値：2（改善が実施されないことによるサイバー攻撃被害）	評価値：1（マルウェア等の侵入による脆弱性を突いた広域感染）	評価値：3（顧客提供サービスでの重大インシデント発生）
対応の優先度	評価値：優先度 中	評価値：優先度 低	評価値：優先度 高

上記の例では，DE.CM-8（脆弱性スキャン実施）の適用範囲に関して，③顧客向けITサービスにおけるリスクの低減を重要と捉え，改善策（DevSecOpsやクラウドサービスによる脆弱性スキャンの効率化検討）の優先度を高に設定している．

3. 4. 4　対応（RS）

CSFにおける対応（RS）は，サイバーセキュリティインシデントに円滑に対応するための領域であり，そのカテゴリは，対応計画（RP），コミュニケーション（CO），分析（AN），影響の緩和（MI），改善（IM）といった内容で構成されている．組織において発生したインシデントに対応するための一般的にCSIRT（Computer Security Incident Response Team）と呼ばれるセキュリティ事故対応チームが主管する機能が含まれている領域であり，各カテゴリの配下に位置するサブカテゴリ数は合計で16項目が存在する．セキュリティインシデントへの対応計画を定め，実際にインシデントが発生した際にはCSIRT内や関連部門，他組織CSIRTや外部機関とも連携して，発生したインシデントの影響を緩和し，インシデントからの学習を通じて対応活動の改善を図ることが対応（RS）領域の目的となる．フレームワークコアの中でもセキュリティの専門知識と経験を要する領域であり，近年のインシデントの多発を受け，組織内にCSIRTを設置する企業も急増している．CSIRT間連携のセキュリティ団体である日本シーサート協議会[*8]への加盟会員数は，2019年5月時点において350チームを超えている．完全な事前防御が難しいサイバーセキュリティインシデントの特性を踏まえ，インシデント対応力の強化に対するニーズが急速な高まりを見せている．

対応（RS）におけるアセスメント例（RS.AN-3：フォレンジックの実施）は表9の通りである．

表9　アセスメント例（対応（RS.AN-3：フォレンジックの実施））

カテゴリ：RS.AN	**分析**：適切な対応を確実にし，復旧活動を支援するために，分析を実施している		
サブカテゴリ：RS.AN-3	フォレンジック[*9]を実施している		
情報資産（適用対象）	①フォレンジック技術者	②フォレンジック検証環境	③セキュリティ専門ベンダー
主管部署	CSIRT	CSIRT	CSIRT
現状	フォレンジックツールを導入し，トレーニングを実施している．	CSIRTの個別環境にてフォレンジックを実施している．	フォレンジックを委託可能なセキュリティ専門ベンダーを複数選定している．
主要な課題	CSIRT内において，ツールを扱える要員が限定的である．	フォレンジック専用の充分な規模の検証環境を整備すること．	フォレンジックの委託において発生するコストを低減すること．
課題に対する対策	CSIRT全体へフォレンジック技術を展開，共有する．	クラウドサービスを活用し，より高度なフォレンジック用環境を整備する．	状況に応じて，サイバーセキュリティ保険の適用等も検討する．
成熟度評価	評価値：2（リスク情報を活用している：Risk Informed） ※フォレンジック関連の人材育成，環境整備を拡大する		

現状のリスク	評価値：3（大規模，複数インシデント発生時のフォレンジック要員不足）	評価値：3（フォレンジック作業の遅延）	評価値：2（フォレンジック作業のコスト増加）
対応の優先度	評価値：優先度 高	評価値：優先度 高	評価値：優先度 中

上記の例では，RS.AN-3（フォレンジック実施）に関して，②フォレンジック技術者，③フォレンジック検証環境におけるリソース不足のリスク低減を重要と捉え，改善策（フォレンジック実施の環境整備強化）の優先度を高に設定している．

3. 4. 5　復旧（RC）

CSF における復旧（RC）は，セキュリティインシデントにより影響を受けた事業を円滑に復旧させるための領域であり，そのカテゴリは，復旧計画（RP），改善（IP），コミュニケーション（CO）といった内容で構成されている．対応（RS）の領域と同様に，組織において発生したインシデントに対応するための一般的に CSIRT と呼ばれるセキュリティ事故対応部門や組織の広報活動を主管する部門の要件が含まれている領域である．各カテゴリの配下に位置するサブカテゴリ数は合計で 6 項目が存在する．セキュリティインシデントの復旧計画を定め，実際にインシデントが発生した際には CSIRT，広報部門，リスク管理部門と連携し，発生したインシデントをクローズすると共に，インシデントにより発生した組織のダメージを回復させ，インシデントからの学習を通じて復旧活動の改善を図ることが復旧（RC）領域の目的である．前項の対応（RS）と両輪で扱われるインシデント対応の領域の一部である．

復旧（RC）におけるアセスメント例（RC.RP-1：復旧計画の実施）は表 10 の通りである．

表 10　アセスメント例（復旧（RC.RP-1：復旧計画の実施））

カテゴリ：RC.RP	**復旧計画**：サイバーセキュリティインシデントによる影響を受けたシステムや資産を復旧できるよう，復旧プロセスおよび手順を実施し，維持している
サブカテゴリ：RC.RP-1	イベントの発生中または発生後に復旧計画を実施している
情報資産（適用対象）	インシデント対応マニュアルに基づく，対応復旧計画およびプロセス
主管部署	セキュリティ管理部門
現状	インシデントが発生した場合，インシデント対応マニュアルの記載に基づき，事案個別の対応復旧計画を策定，リスク対策会議の場において，進捗や課題の管理を実施している．（対応中においても計画の適宜見直しを図っている）
主要な課題	発生したインシデントの種類，範囲，影響度等により，対応復旧計画の細部が異なるため，完全な標準化や事前の手順化が困難である．
課題に対する対策	より迅速な対応復旧を図るため，インシデント対応マニュアルの改善や周知，机上演習，情報共有等を継続する．
成熟度評価	評価値：3（繰り返し適用可能である：Repeatable） ※インシデント対応復旧の基本プロセスは確立しており，細部の継続改善を図ることでブラッシュアップする

現状のリスク	評価値：2（発生したインシデントの復旧段階において，ダメージを軽減できず，影響が拡大する）
対応の優先度	評価値：優先度 中

上記の例では，RC.RP-1（復旧計画の実施）に関して，復旧計画のベースとなるインシデント対応マニュアル等の不十分さに起因するインシデントの長期化やダメージ回復の失敗に対するリスク低減を重要と捉え，改善策（インシデント対応プロセスの改善や継続的な演習等による習熟および情報共有の強化）の優先度を中に設定している．

3.5　アセスメント結果の報告と実行計画

アセスメントの結果を関連部署や経営層に報告，共有することは極めて重要なプロセスである．アセスメントシートに加え，CSF フレームワークコアの一覧や導出した詳細な実行計画に相当する WBS（Work Breakdown Structure）等を添付する．経営層への報告に際しては，現状の成熟度やリスクの大きさ等をレーダーチャートなどを用い，できる限りビジュアルかつ平易に伝える．CSF のサブカテゴリを基軸とする詳細な評価結果に加えて，IPA（独立行政法人情報処理推進機構）が毎年公表している「情報セキュリティ 10 大脅威」[4]への対応状況などを付記してわかり易く説明することも有効である．立案した実行計画を確実に実施して効果を管理し，次回のアセスメントにおいてその効果を成熟度指標に基づき再評価することにより，アセスメントから改善計画の実行およびその確認までの継続的サイクルをサイバーセキュリティ経営の活動に埋め込み，組織におけるセキュリティ文化に浸透させていくのである．

4.　サイバーセキュリティリスクの継続的低減

サイバーセキュリティにおけるアセスメントとはあくまでもリスクを評価し実行計画を策定するための作業であり，アセスメントを実施することが最終目的ではない．アセスメントに基づく実行計画として，「誰が，いつまでに，どのような手段で，何を実施するか」を明確に定め，プロジェクト管理の観点でその活動を可視化した上で，サイバーセキュリティのリスク対応活動を確実に実行し，リスク低減に寄与することがアセスメント実施の最終目的である．また，今回紹介した広範に及ぶ包括的なアセスメントについては，定期的に実施することが望ましいが，アセスメント自体に係る作業負荷や導出したリスク対応策の実施対応期間，アセスメントで使用するガイドラインやフレームワークの改訂状況等も踏まえ，実施サイクルを適切に設定するべきである．実施サイクルを短く設定し過ぎると，運用負荷が増し，アセスメントそのものの形骸化を招くこともある．様々な脅威や脆弱性，インシデントなどのセキュリティ情報の継続的な収集や共有がなされ，ハイリスクなインターネット接続やアプリケーションサービスに対するセキュリティ点検や脆弱性スキャン，重要情報の漏えい監視等のモニタリングを行い，CSIRT 等のインシデント対応体制を整備することにより，定常的にセキュリティリスクを低減することができる．自組織で対応できない部分については，外部のセキュリティ関連サービスを活用するなどの柔軟な判断が求められる．アセスメントで使用したサイバーセキュリティフレームワークは，事前の防御対策に限らず，日々変化するサイバー脅威や脆弱性，インシデントの検知や対応といったサイバーセキュリティの本質的対応に向けた全体の枠組みを提供するものであり，既に ISMS 認証等を取得し，情報セキュリティ管理の PDCA サイクル

を回している組織においても，サイバーセキュリティへの適合という経営課題に関して活用する価値が高い．

5. お わ り に

日々変化するセキュリティの脅威や脆弱性，発生するインシデントへの対応を継続すると共に，本稿で紹介したアセスメントに基づき，中長期の方針や計画を維持し，経営層とも共有しながら自社のサイバーセキュリティを段階的に成熟させていく．サイバーセキュリティの対応には，投資効果の明確化，管理面と技術面や事前対策と事後対策のバランス確保，全ての施策のベースとなる人材の育成といった困難な課題が存在するが，継続性を保ち改善していく．

最後にサイバーセキュリティの様々な活動は，特定のセキュリティ関連部門だけでなく，経営から現場に至る多数の関連部署の協力により成立している．日本ユニシスグループのサイバーセキュリティに関わる全ての関係各位に深く感謝申し上げる．

＊1　日々発生する脆弱性情報をモニタリング，分析，情報共有するための一連のプロセス
＊2　サイバー脅威の防止や検知に利用できる情報（マルウェア，有害サイト等）の総称
＊3　サイバーセキュリティの技術を習得するためのセキュリティコンテスト（CTF：Capture The Flag）
＊4　サイバーセキュリティインシデントへの対応力を高めるための机上あるいは実践的訓練
＊5　パターンファイルやシグネチャに依存せず，既知および未知の攻撃やマルウェアに対応する機能（防御，検知）を備えた新しいエンドポイントセキュリティ製品
＊6　システム基盤やアプリケーションの脆弱性を検出するためのセキュリティ診断プロセス
＊7　開発（Dev：Development）および運用（Ops：Operations）の職務と，セキュリティ（Sec：Security）の職務とを統合し，開発段階からセキュリティを考慮することで安全なアプリケーションを高速開発，運用するための仕組み
＊8　日本コンピュータセキュリティインシデント対応チーム協議会：https://www.nca.gr.jp/
＊9　不正アクセスや機密情報漏えいなどのサイバーセキュリティインシデント発生時におけるログ解析や流出した情報を特定するためのデジタル鑑識技術

参考文献
［1］ NIST Cybersecurity Framework, National Institute of Standards and Technology，April 16, 2018　https://www.nist.gov/cyberframework
［2］「重要インフラのサイバーセキュリティを改善するためのフレームワーク　1.1 版」（NIST Cybersecurity Framework 和訳），独立行政法人情報処理推進機構（IPA），2019 年 1 月　https://www.ipa.go.jp/security/publications/nist/index.html
［3］ The CIS Critical Security Controls for Effective Cyber Defense Version6.1，「効果的なサイバー防御のための CIS クリティカルセキュリティコントロール」，Center for Internet Security，2015 年 10 月
https://www.cisecurity.org/wp-content/uploads/2017/03/CIS-CSC_v6.1_Japanese_Final_r1.pdf
［4］「情報セキュリティ 10 大脅威 2019」，独立行政法人情報処理推進機構（IPA），2019 年 7 月　https://www.ipa.go.jp/security/vuln/10threats2019.html

※上記注釈及び参考文献に含まれる URL のリンク先は，2019 年 7 月 31 日時点での存在を確認．

執筆者紹介　福　田　俊　介（Shunsuke Fukuda）

1990年日本ユニシス(株)中途入社．主に金融機関向けネットワーク構築，EC サイトにおけるインターネット接続基盤構築，セキュリティコンサルティングサービスに従事．日本ユニシスグループ・サイバーセキュリティ戦略推進プロジェクト，CSIRT（セキュリティインシデント対応チーム）メンバー．