セキュリティ対応組織（SOC/CSIRT）の教科書

～ X.1060 フレームワークの活用 ～

別紙：FIRST CSIRT Services Framework とのマッピング

第 3.2.1 版

2025 年 10 月 17 日

NPO 日本ネットワークセキュリティ協会 （JNSA）

日本セキュリティオペレーション事業者協議会 （ISOG-J）

改版履歴

2016/11/25	初版作成
2017/10/03	第２．０版作成
2018/03/30	第２．１版作成
2023/2/13	第３．０版作成
2023/10/17	第３．１版作成
2024/10/17	第３．２版作成
2025/10/17	第３．２．１版作成 ハンドブック、ハンドブックの別紙を追加 別紙：FIRST CSIRT Services Framework とのマッピングを追加

免責事項

- 本資料の著作権は日本セキュリティオペレーション事業者協議会(以下、ISOG-J)に帰属します。
- 引用については、著作権法で引用の目的上正当な範囲内で行われることを認めます。引用部分を明確にし、出典が明記されるなどです。
- なお、引用の範囲を超えると思われる場合は ISOG-J へご相談ください(info (at) isog-j.org　まで)。
- 本文書に登場する会社名、製品名、サービス名は、一般に各社の登録商標または商標です。本文中では®や TM、©マークは明記していません。
- ISOG-J ならびに執筆関係者は、このガイド文書に関するいかなる責任も負うものではありません。全ては自己責任にてご活用ください。

目次

1. FIRST CSIRT Services Framework Version 2.1.0 とのマッピング

X.1060		FIRST CSIRT Services Framework version 2.1.0		
サービス	概要	サービス	機能	目的
A-1. リスクマネジメント	「リスクマネジメント」サービスは、リスクに対して組織を方向づけ、コントロールできるよう、A-2 から A-13 を含む統括的な活動を実現する。	N/A		
A-2. リスクアセスメント	「リスクアセスメント」サービスは、組織の資産や脅威、セキュリティ対策の観点から、組織のリスクレベル把握を実現する。	9.4 サービス:技術およびポリシーに関するアドバイス	9.4.1 機能:リスクマネジメント支援	情報セキュリティおよびその他の関連機能と連携して、機会と脅威の特定能力を改善し、統制・管理を改善し、損失防止およびインシデントマネジメントを改善する。
A-3. ポリシーの企画立案	「ポリシーの企画立案」サービスは、具体的なセキュリティポリシーの定義や、ガイドラインの作成に関するすべての活動を支援する。	7.5 サービス:脆弱性の開示	7.5.1 機能:脆弱性開示ポリシーとインフラストラクチャの整備	CSIRT が脆弱性をハンドリングして開示する方法、および脆弱性を開示するために使用されるメカニズムについて、フレームワークを提供し、期待値を設定するポリシーを策定し、維持する。
		8.1 サービス:デ	8.1.1 機能:ポリシーの集約、	インフラで何が起きている（と考えら

		ータ取得	抽出、ガイダンス	れる）のか把握するためにコンスティチュエンシーおよびその資産が準拠すべきコンテキストを確立する。
		9.4 サービス:技術およびポリシーに関するアドバイス	9.4.3 機能:ポリシーの支援	アドバイスが利用される可能性のある環境および適用されるリソースの制約を考慮し、公平で事実に基づいたアドバイスを提供することにより、ポリシーの開発および実施について信頼されるアドバイザーとして行動する。
A-4. ポリシー管理	「ポリシー管理」サービスは、ポリシーや組織の規定を評価して定期的に見直しや、新たな外部要件（例えば、規制やガイドライン）への準拠を実現する。	N/A		
A-5. 事業継続性	「事業継続性」サービスは、組織の事業継続計画の実現や実行が正しく行われるために必要な経営上の機能を支援する。	9.4 サービス:技術およびポリシーに関するアドバイス	9.4.2 機能:事業継続および災害復旧計画の支援	事業継続と災害復旧に関する信頼されるアドバイザーとして、中立的で事実に基づいたアドバイスを提供し、そのアドバイスを使用できる環境と適用されるリソースの制約を考慮する。
A-6. 事業影響度分析	「事業影響度分析」のサービスは、様々なイベントや	N/A		

	シナリオから起こり得る影響の体系的なアセスメントを実現する。このサービスは、発生しうる損失の規模を組織が理解するのに役立つ。直接的な金銭的損失だけでなく、利害関係者の信頼喪失や風評被害など、その他の影響も対象となる場合もある。			
A-7. リソース管理	「リソース管理」サービスは、各種セキュリティ活動を支えるリソース（人、予算、システムなど）計画と、各サービスへの適切な割り当てを実現する。	N/A		
A-8. セキュリティアーキテクチャ設計	「セキュリティアーキテクチャ設計」サービスは、ビジネスをセキュアにするためのアーキテクチャの確立を実現する。システムの設計やビジネスプロセスの制約（例えば、 サプライチェー	N/A		

	ン）を考慮した各種セキュリティ対策をまとめ、CDCのプラットフォーム（カテゴリーG にあるような）の開発や維持を実現する。			
A-9. トリアージ基準管理	「トリアージ基準管理」サービスは、全社のポリシーで合意された範囲内で発覚した事象（例えば、インシデント、脆弱性の発覚、脅威情報の発見など）へのトリアージ（対応の優先順位）基準作成を実現する。	N/A		
A-10. 対応策選定	「対応策選定」サービスは、A-9 のトリアージ基準に対する対応策や、各種のセキュリティ対策に最も適切な技術の選定活動を支援する。	N/A		
A-11. 品質管理	「品質管理」サービスは、セキュリティ活動の品質に問題がないかどうか、ビジネスに悪影響を与えていない	N/A		

	かどうか（ユーザビリティ、生産性など）の一定期間（1週間、1 ヶ月など）ごとの点検を実施する。			
A-12. セキュリティ監査	「セキュリティ監査」サービスは、組織が特定の拠点や期間において、セキュリティポリシーや統制をどのように実現しているかの体系的かつ定量的な監査を実現する。CDC 関係者は、必要な情報の統制の実施状況の証拠を提供するために、監査活動に間接的に関与する。	N/A		
A-13. 認証	「認証」サービスは、組織がさまざまな規格や認証スキームの適合に向けた活動を支援する。	N/A		
B-1. リアルタイム監視	「リアルタイム監視」サービスは、ログやネットワークフローからシステムの状態や不審な動きを監視・分	5.2 サービス:イベント分析	5.2.1 機能:関連付け	他の潜在的または進行中のセキュリティインシデントに直接関連するイベントを特定する。

	析し、インシデントやイベントに応じて必要な情報を収集し、トリアージを支援する。			
			5.2.2 機能:適格性確認	真陽性の検知を特定、分類し、優先順位付けするために、検知された潜在的な情報セキュリティインシデントをトリアージして適格性を確認する。
		8.2 サービス:分析と統合	8.2.2 機能:イベント検知(アラートや探索を通じて)	コンスティチュエンシーの現在の状況の詳細を断定し、確認する。
B-2. イベントデータ保管	「イベントデータ保管」サービスは、セキュリティ監視や分析で収集されたイベントを集約し、一元的な保管を実現する。	N/A		
B-3. 通知・警告	「通知・警告」サービスは、情報資産に対する潜在的なリスクがハイライトされたイベント（セキュリティ機器の警告、セキュリティ速報、脆弱性、拡散する脅威など）を、関係する内部で役目を持ったものへの通知を実	N/A		

	現する。			
B-4. レポート問い合わせ対応	「レポート問い合わせ対応」サービスは、分析に関するデータやレポートに関する問い合わせ対応を実現する。	N/A		
C-1. フォレンジック分析	「フォレンジック分析」サービスは、何が発生したのかの判断を促進するため、セキュリティ関連資産から収集された、あるいはイベントに関連したデジタル証跡の分析を実現 する。	6.3 サービス:アーティファクトとフォレンジック痕跡の分析	6.3.1 機能: メディアまたはサーフェス分析	アーティファクトから収集された情報を、他のパブリックおよびプライベートのアーティファクトや署名リポジトリと比較する。
C-2. 検体解析	「検体解析」サービスは、フォレンジックの過程で発見された、攻撃者によって設置されたマルウェア、プログラムやスクリプトの解析を実現する。	6.3 サービス:アーティファクトとフォレンジック痕跡の分析	6.3.2 機能:リバース・エンジニアリング	アーティファクトの完全な機能を、その実行環境に関係なく断定するために、アーティファクトの詳細な静的分析を行う。
			6.3.3 機能:ランタイムまたは動的解析	アーティファクトの操作に関する洞察を提供する。
C-3. 追及・追跡	「追及・追跡」サービスは、	6.3 サービス:ア	6.3.4 機能:比較分析	カタログ化されたアーティファクト

	環境に対するあらゆる攻撃の発生源を追及・追跡を実現するもので、これはセキュリティインシデントの抑制や分析の重要な成功要因となる。内部と外部の両方の攻撃者を追及・追跡できる能力（例えば、サイバーアトリビューション）があれば将来の攻撃を事前に防ぐことができる。	ーティファクトとフォレンジック痕跡の分析		のファミリー分析など、共通の機能または意図の特定に重点を置いた分析を行う。
C-4. 証拠収集	「証拠収集」サービスは、扱われたインシデントに関係する電磁的証拠を収集・保全し、証拠としての妥当性の維持を実現する（証拠保全の一貫性）。	N/A		
D-1. インシデント報告受付	「インシデント報告受付」サービスは、運用における分析報告の受け付けを実現する。報告の受領は組織内部からだけではなく、外部の組織からの場合もある。	6.1 サービス:情報セキュリティインシデント報告の受付	6.1.1 機能:情報セキュリティインシデント報告の受理	コンスティチュエンシーまたは第三者から報告された、情報セキュリティインシデントに関する情報を受付または受理する。

D-2. インシデントハンドリング	「インシデントハンドリング」サービスは、受け付けたインシデントに対処し、D-3 から D-7 の活動の調整を実現する。	6.1 サービス:情報セキュリティインシデント報告の受付	6.1.2 機能:情報セキュリティインシデントのトリアージと処理	報告された情報セキュリティインシデントについて、初めにレビュー、分類、優先順位付け、および処理を行う。
		6.5 サービス:情報セキュリティインシデントの調整	6.5.4 機能:活動の調整	すべてのコミュニケーションと活動の状況を追跡する。
		8.2 サービス:分析と統合	8.2.3 機能:情報セキュリティインシデントマネジメントの意思決定支援	被害を抑制し、将来のリスクを緩和する、あるいは新しく発生した弱点を特定するのに役立つかもしれない新しい見識をインシデント中に特定する。
			8.2.4 機能:状況的影響	現在観察されている事象や今後観察されうる事象が状況図に与えると予想される潜在的影響を決定する。
D-3. インシデント分類	「インシデント分類」サービスは、発生したインシデントとその原因の種別について共通理解を促すために、インシデントの分類を実現する。	6.2 サービス:情報セキュリティインシデントの分析	6.2.1 機能:情報セキュリティインシデントのトリアージ(優先順位付けと分類)	情報セキュリティインシデントを分類し、優先順位を付け、初期評価を行う。
			6.2.2 機能:情報収集	情報セキュリティインシデントおよ

				びその一部とみなされるすべての情報セキュリティイベントに関連する情報を取得し、カタログを作成し、保存および追跡する。
			6.2.3 機能:詳細分析の調整	インシデントに関するその他の技術分析を開始して追跡する。
D-4. インシデント対応・封じ込め	「インシデント対応・封じ込め」サービスは、インシデントがすべてのリソースに広がるなど、被害や影響が拡大する前の封じ込めを実現する。	6.2 サービス:情報セキュリティインシデントの分析	6.2.4 機能:情報セキュリティインシデントの根本原因分析	インシデントの根本原因を特定するため、悪用された脆弱性が存在したり、悪用が成功したりするのを許してしまった状況(ユーザーの行動を含むが、それに限定されない)を特定する。
		6.4 サービス:緩和と回復	6.4.1 機能:対応計画の策定	影響を受けたシステムの完全性を回復し、影響を受けたデータ、システム、およびネットワークを劣化していない動作状態に戻し、元のセキュリティ問題が再び悪用されるコンテキストを再生することなく、影響を受けたサービスを完全な機能に復元する計画を定義して実施する。
			6.4.2 機能:一時的な対策と封じ込め	情報セキュリティインシデントがこれ以上拡大しない、すなわち、現在影響を受けているシステムやユーザー、

				ドメインに限定して、これ以上の損失(文書の漏えい、データベースまたはデータの変更等を含む)が発生することがないように保証する対策を実施する。
D-5. インシデント復旧	「インシデント復旧」サービスは、対象となるシステムを通常状態へ回復することを支援する。	6.4 サービス:緩和と回復	6.4.3 機能:システムの復旧	影響を受けたドメインやインフラストラクチャ、ネットワークの修復および、同様の活動の再発防止に必要な変更を行う。
			6.4.4 機能:他の情報セキュリティエンティティの支援	情報セキュリティインシデントを適切に緩和し、また情報セキュリティインシデントから回復するために必要な管理および技術的活動を、コンスティチュエンシーが実行できるようにする。
D-6. インシデント通知	「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。	6.5 サービス:情報セキュリティインシデントの調整	6.5.1 機能:コミュニケーション	利害関係者と効果的に連携し、必要とされる機密性を提供する、適切な複数のコミュニケーションチャネルを確立する。
			6.5.2 機能:通知の配信	情報セキュリティインシデントの影響を受けるエンティティ、またはイン

				シデントへの対応に貢献できるエンティティにアラートを送る。また、これらのエンティティに対して、それぞれの役割や、期待される可能性のある協力や支援について理解してもらうのに必要な情報を提供する。
			6.5.3 機能:関連情報の配信	特定されたエンティティとのコミュニケーションを維持し、それらのエンティティが利用可能な洞察と教訓から利益を得たり、改善された対応を適用したり、新たなアドホックな措置を講じたりできるようにするために、利用可能な情報の適切な流れを提供する。
		6.6 サービス:危機管理支援	6.6.1 機能:コンスティチュエンシーへの情報配信	危機への対処を支援するために確立されたコミュニケーションリソースを提供する。
			6.6.2 機能:情報セキュリティの状況報告	危機管理チームが、現在の情報セキュリティインシデントと既知の脆弱性の完全な概要を把握し、これを全体的な優先事項と戦略の一部として検討できるようにする。
			6.6.3 機能:戦略的意思決定	現在起きている情報セキュリティイ

			の伝達	ンシデントに対して危機が与える影響について、他のエンティティにタイムリーに情報提供する。
		7.1 サービス:脆弱性の発見・調査	7.1.1 機能:インシデント対応の脆弱性発見	セキュリティインシデントの一部として悪用された脆弱性を特定する。
D-7. インシデント対応報告	「インシデント対応報告」サービスは、対応が完了したインシデントのレポートの完成と報告を実現する（対策の試みが長期化する場合は、CDC の戦略マネジメント（カテゴリーA）に引き継がれる)。インシデント対応中に CDC 関係者が現状報告を必要とする場合は、中間報告を行う。	6.5 サービス:情報セキュリティインシデントの調整	6.5.5 機能:報告	次のステップに関するさらなる決定が、その時点で可能な最良の状況把握に基づくよう、事業内のすべての関係エンティティが、確実に現在の活動状況に関する情報を持っているようにする。
			6.5.6 機能:メディアとのコミュニケーション	風評や誤解を招くような情報の流布を避けるために、進行中のイベントに関する正確で分かりやすい、事実に基づいた情報を提供できるように(公共の)メディアと連携する。
		8.3 サービス:コミュニケーショ	8.3.2 機能:報告と推奨事項	結果、アーティファクトまたは所見を作成し、分析中に発見または作成され

		ン		た重大な情報を、受取手が理解できる方法と形式で伝える。
E-1. ネットワーク情報収集	「ネットワーク情報収集」サービスは、保護対象となるネットワーク構成の概要の収集を実現する。	N/A		
E-2. 資産棚卸	「資産棚卸」サービスは、CDC の所掌範囲となるビジネスインフラ全体を構成するシステム、アセット、アプリケーションの全数調査の情報管理を実現する。	8.1 サービス:データ取得	8.1.2 機能:機能、役割、アクション、主要リスクへの資産のマッピング	既存の資産、コンスティチュエンシー、ベースラインおよび期待される活動の知識を提供することで、異常な状況の観察を特定する分析機能を支援する。
E-3. 脆弱性診断	「脆弱性診断」サービスは、ネットワーク、システム、アプリケーションの脆弱性を特定し、その脆弱性がどのように悪用されるか判断するとともに、リスクをどのように軽減できるかの提案を実現する。	7.1 サービス:脆弱性の発見・調査	7.1.3 機能:脆弱性調査	意図的な活動または調査の結果として、新しい脆弱性を発見または探索する。
		7.6 サービス:脆弱性対応	7.6.1 機能:脆弱性の検知・スキャン	設置されたシステムに既知の脆弱性が存在するかどうかの調査に積極的に取り組む。

E-4. パッチ管理	「パッチ管理」サービスは、情報技術(IT)サービスの可用性を維持しながら、必要なセキュリティパッチのインストールを支援する。	7.6 サービス:脆弱性対応	7.6.2 機能:脆弱性の修正	脆弱性が悪用されないようにするために脆弱性を修正または緩和する。通常は、ベンダーが提供するパッチまたはその他のソリューションをタイムリーに適用する。
E-5. ペネトレーションテスト	「ペネトレーションテスト」サービスは、攻撃者に悪用される可能性のあるセキュリティの脆弱性を明らかにし、考えられる侵害方法の炙り出しを実現する。（例：脅威ベースのペネトレーションテスト)。	7.6 サービス:脆弱性対応	7.6.1 機能:脆弱性の検知・スキャン	設置されたシステムに既知の脆弱性が存在するかどうかの調査に積極的に取り組む。
E-6. 高度サイバー攻撃耐性評価	高度サイバー攻撃(APT)に対抗するための「高度サイバー攻撃耐性評価」サービスは、標的型メール訓練やソーシャルエンジニアリングテストを実施しながら、標的型攻撃に対する組織耐性の計測を実現する。	9.3 サービス:演習	9.3.1 機能:要件分析	演習の、あらかじめ決められた範囲と焦点の特定の課題に集中することにより、確実に十分な成果を得られるようにする。
			9.3.2 機能:フォーマットと環境の開発	演習の実施に必要な内部および外部のリソースとインフラストラクチャ

				を特定および決定する。
			9.3.3 機能:シナリオ開発	コミュニケーションの観点を含む、模擬サイバーセキュリティイベントやインシデントのハンドリングを通して、そのサービスと機能の効率と有効性、およびそのスキル、知識、能力を改善する機会を対象者に提供する。
			9.3.4 機能:演習の実行	CSIRT チームが組織の CSIRT 計画の妥当性とその実行能力に対する信頼を高めるためにドリル・演習を実施する。
			9.3.5 機能:演習成果レビュー	実際の観察に基づいて、演習の形式的で客観的な分析を行う。
E-7. サイバー攻撃対応力評価	「サイバー攻撃対応力評価」サービスは、攻撃発生を想定したシナリオに基づき、セキュリティ対応が実際に発動され、インシデントを遅滞なく終息させることができるかどうかの確認を実現する（サイバー攻撃対応演習と呼ぶ)。	9.3 サービス:演習	9.3.1 機能:要件分析	演習の、あらかじめ決められた範囲と焦点の特定の課題に集中することにより、確実に十分な成果を得られるようにする。
			9.3.2 機能:フォーマットと	演習の実施に必要な内部および外部

			環境の開発	のリソースとインフラストラクチャを特定および決定する。
			9.3.3 機能:シナリオ開発	コミュニケーションの観点を含む、模擬サイバーセキュリティイベントやインシデントのハンドリングを通して、そのサービスと機能の効率と有効性、およびそのスキル、知識、能力を改善する機会を対象者に提供する。
			9.3.4 機能:演習の実行	CSIRT チームが組織の CSIRT 計画の妥当性とその実行能力に対する信頼を高めるためにドリル・演習を実施する。
			9.3.5 機能:演習成果レビュー	実際の観察に基づいて、演習の形式的で客観的な分析を行う。
E-8. ポリシー遵守	「ポリシー遵守」サービスは、事前に定義されたセキュリティポリシーへの適合性と遵守の検証を支援する。	N/A		
E-9. 堅牢化	「堅牢化」サービスは、システムに対するセキュリティ設定の見極めや評価、適用するため、および攻撃のリ	N/A		

	スクの低減や排除のための、IT コンポーネントの構成最適化を実現する。			
F-1. 事後分析	「事後分析」サービスは、CDC 関係者の手順やツールの見直しや改善を実現するため、インシデントの解決法の詳述を実現する。	5.1 サービス:監視と検知	5.1.2 機能:検知ユースケース管理	検知ユースケースのポートフォリオを、ライフサイクル全体を通して管理する。
		6.2 サービス:情報セキュリティインシデントの分析	6.2.5 機能:クロスインシデント相関	利用可能なすべての情報を使って、コンテキストを最大限に理解し、それ以外の方法では認識されなかった、または対処できなかった相互関係を検知できるようにする。
F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。	6.3 サービス:アーティファクトとフォレンジック痕跡の分析	6.3.4 機能:比較分析	カタログ化されたアーティファクトのファミリー分析など、共通の機能または意図の特定に重点を置いた分析を行う。
		7.1 サービス:脆弱性の発見・調査	7.1.1 機能:インシデント対応の脆弱性発見	セキュリティインシデントの一部として悪用された脆弱性を特定する。
		7.2 サービス:脆弱性報告の取得	7.2.1 機能:脆弱性報告の受理	コンスティチュエンシーまたは第三者から報告された脆弱性に関する情

				報を受付または受理する。
			7.2.2 機能:脆弱性報告のトリアージと処理	脆弱性報告の初期レビュー、分類、優先順位付け、および処理を行う。
		7.3 サービス:脆弱性分析	7.3.1 機能:脆弱性のトリアージ(検証と分類)	脆弱性を分類し、優先順位を付け、初期評価を行う。
			7.3.2 機能:脆弱性の根本原因分析	脆弱性の原因となった、またはその存在を顕在化する設計上または実装上の欠陥を理解する。
			7.3.3 機能:脆弱性対策開発	潜在的な脆弱性を修正(是正)するため、または脆弱性が悪用される影響を緩和(軽減)するために必要な手順を開発する。
		8.1 サービス:データ取得	8.1.3 機能:収集	分析・解釈サービスや他の CSIRT サービスを支援するために情報を収集する。
		8.2 サービス:分析と統合	8.2.1 機能:予測と推定	現在の状況の特定または将来の状況の予測を目的として、データ取得中に収集された情報を分析する。
F-3. 外部脅威情報の収集・評価	「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外	7.1 サービス:脆弱性の発見・調査	7.1.2 機能:公的情報源による脆弱性の発見	公的情報源またはその他の第三者の情報源を参照して、新しい脆弱性について知る

	部情報）の収集を実現する。			
		7.2 サービス:脆弱性報告の取得	7.2.1 機能:脆弱性報告の受理	コンスティチュエンシーまたは第三者から報告された脆弱性に関する情報を受付または受理する。
			7.2.2 機能:脆弱性報告のトリアージと処理	脆弱性報告の初期レビュー、分類、優先順位付け、および処理を行う。
		7.3 サービス:脆弱性分析	7.3.1 機能:脆弱性のトリアージ(検証と分類)	脆弱性を分類し、優先順位を付け、初期評価を行う。
			7.3.2 機能:脆弱性の根本原因分析	脆弱性の原因となった、またはその存在を顕在化する設計上または実装上の欠陥を理解する。
			7.3.3 機能:脆弱性対策開発	潜在的な脆弱性を修正(是正)するため、または脆弱性が悪用される影響を緩和(軽減)するために必要な手順を開発する。
		8.1 サービス:データ取得	8.1.3 機能:収集	分析・解釈サービスや他の CSIRT サービスを支援するために情報を収集する。
		8.2 サービス:分析と統合	8.2.1 機能:予測と推定	現在の状況の特定または将来の状況の予測を目的として、データ取得中に収集された情報を分析する。
F-4. 脅威情報報告	「脅威情報報告」サービスは、内部と外部の脅威情報	7.3 サービス:脆弱性分析	7.3.3 機能:脆弱性対策開発	潜在的な脆弱性を修正(是正)するため、または脆弱性が悪用される影響を

	を取りまとめ、詳細も含めたドキュメント化を実現する。			緩和(軽減)するために必要な手順を開発する。
		8.3 サービス:コミュニケーション	8.3.2 機能:報告と推奨事項	結果、アーティファクトまたは所見を作成し、分析中に発見または作成された重大な情報を、受取手が理解できる方法と形式で伝える。
F-5. 脅威情報の活用	「脅威情報の活用」サービスは、あらゆるカテゴリーのセキュリティ対応のために、脅威情報の編纂と発信を実現する。	7.5 サービス:脆弱性の開示	7.5.2 機能:脆弱性の公表・連絡・周知	脆弱性を検知、修正、または緩和し、将来の脆弱性の不正利用を防止できるようにコンスティチュエンシー(または一般の人々)に情報を提供する。
			7.5.3 機能:脆弱性開示後のフィードバック	脆弱性の開示または文書に関する、コンスティチュエンシーからの質問または報告を受領し、回答する。
		8.1 サービス:データ取得	8.1.4 機能:データ処理と準備	CSIRT 活動および分析サービスの要件をサポートできる、信頼性と一貫性のある最新のデータセットを確立する。
G-1. セキュリティアーキテクチャ実装	「セキュリティアーキテクチャ実装」サービスは、CDCの戦略マネジメント（カテゴリーA）で設計したセキュ	5.1 サービス:監視と検知	5.1.1 機能:ログとセンサーの管理	ログソースとセンサーを管理する。

	リティアーキテクチャの実装を実現する。			
		8.3 サービス:コミュニケーション	8.3.3 機能:実装	状況の変化に対してさらなる準備や対応をするためにコミュニケーションに基づいてコンスティチュエンシーの環境を調整する。
G-2. ネットワークセキュリティ製品基本運用	「ネットワークセキュリティ製品基本運用」サービスは、ファイアウォール、不正侵入検知システム/不正侵入防止システム(IDS/IPS)、WAF、プロキシなどのネットワーク装置の運用を実現する。	5.1 サービス:監視と検知	5.1.1 機能:ログとセンサーの管理	ログソースとセンサーを管理する。
G-3. ネットワークセキュリティ製品高度運用	「ネットワークセキュリティ製品高度運用」サービスは、IDS/IPS や WAF などの攻撃検知機能を持った製品において、製品ベンダーの検知シグネチャでは不十分な場合に、組織独自のカスタムシグネチャ作成を実現する。	5.1 サービス:監視と検知	5.1.2 機能:検知ユースケース管理	検知ユースケースのポートフォリオを、ライフサイクル全体を通して管理する。

			5.1.3 機能:コンテキストデータ管理	検知および強化のためのコンテキストデータソースを管理する。
		8.3 サービス:コミュニケーション	8.3.3 機能:実装	状況の変化に対してさらなる準備や対応をするためにコミュニケーションに基づいてコンスティチュエンシーの環境を調整する。
G-4. エンドポイントセキュリティ製品基本運	「エンドポイントセキュリティ製品基本運用」サービスは、アンチウイルスソフトのようなエンドポイントでの対策製品の運用を実現する。	5.1 サービス:監視と検知	5.1.1 機能:ログとセンサーの管理	ログソースとセンサーを管理する。
G-5. エンドポイントセキュリティ製品高度運用	「エンドポイントセキュリティ製品高度運用」サービスは、エンドポイント内の不審なプログラム挙動を検出し、レジストリの状態やプロセスの実行状況などを収集・分析するエンドポイント対策製品の運用を実現する、必要に応じて、独自にIOC(Indicators of Compromise)を定義し、エ	5.1 サービス:監視と検知	5.1.2 機能:検知ユースケース管理	検知ユースケースのポートフォリオを、ライフサイクル全体を通して管理する。

	ンドポイントでの検知を実現する。			
			5.1.3 機能:コンテキストデータ管理	検知および強化のためのコンテキストデータソースを管理する。
		8.3 サービス:コミュニケーション	8.3.3 機能:実装	状況の変化に対してさらなる準備や対応をするためにコミュニケーションに基づいてコンスティチュエンシーの環境を調整する。
G-6. クラウドセキュリティ製品基本運用	「クラウドセキュリティ製品基本運用」サービスは、クラウドで提供されるセキュリティサービスの運用を実現する。	5.1 サービス:監視と検知	5.1.1 機能:ログとセンサーの管理	ログソースとセンサーを管理する。
G-7. クラウドセキュリティ製品高度運用	「クラウドセキュリティ製品高度運用」サービスは、攻撃検知機能を持つクラウド上のセキュリティサービスに対して、組織独自のカスタムシグネチャ作成を実現する。ベンダーが提供するシグネチャでは不十分な場合に、そのカスタムシグネチャを適用する。	5.1 サービス:監視と検知	5.1.2 機能:検知ユースケース管理	検知ユースケースのポートフォリオを、ライフサイクル全体を通して管理する。

			5.1.3 機能:コンテキストデータ管理	検知および強化のためのコンテキストデータソースを管理する。
		8.3 サービス:コミュニケーション	8.3.3 機能:実装	状況の変化に対してさらなる準備や対応をするためにコミュニケーションに基づいてコンスティチュエンシーの環境を調整する。
G-8. 深掘分析ツール運用	「深堀分析ツール運用」サービスは、デジタルフォレンジックや、マルウェア解析のような深堀分析に用いるツールの運用を実現する。	N/A		
G-9. 分析基盤基本運用	「分析基盤基本運用」サービスは、必要なログデータを蓄積し、日常的に、主にはリアルタイム分析を行うことができる SIEM(Security Information and Event Management)のような分析基盤の運用を実現する。	N/A		
G-10. 分析基盤高度運用	「分析基盤高度運用」サービスは、市販の SIEM では取得できないシステムログ	5.1 サービス:監視と検知	5.1.2 機能:検知ユースケース管理	検知ユースケースのポートフォリオを、ライフサイクル全体を通して管理する。

	やパケットキャプチャデータを保持し、それらのデータやシステムに対して独自の分析アルゴリズムやロジックを開発し、より詳細で正確な分析を組織独自のシステムとして実現する。			
			5.1.3 機能:コンテキストデータ管理	検知および強化のためのコンテキストデータソースを管理する。
G-11. CDC システム運用	「CDC システム運用」サービスは、これまでに記した各種セキュリティ対応ツール、各種レポート作成、問い合わせ対応、脆弱性管理システムなど、セキュリティ対応業務に必要なタスクを遂行するシステムの運用を実現する。	N/A		
G-12. 既設セキュリティツール検証	「既設セキュリティツール検証」サービスは、既に存在するセキュリティ対応ツールのバージョンアップや設定変更時の、システムや運	N/A		

	用への主に可用性の観点での影響検証を実現する。			
G-13. 新規セキュリティツール検証	「新規セキュリティツール検証」サービスは、セキュリティ活動において新たな対策が必要となった場合に、新規のセキュリティ資産の設計・導入を実現する。	7.3 サービス:脆弱性分析	7.3.3 機能:脆弱性対策開発	潜在的な脆弱性を修正(是正)するため、または脆弱性が悪用される影響を緩和(軽減)するために必要な手順を開発する。
H-1. 内部不正対応・分析支援	「内部不正対応・分析支援」サービスは、内部不正が発覚した場合に、セキュリティ活動で取得したログから行動内容を整理することで、組織的な対応を支援する。	6.4 サービス:緩和と回復	6.4.4 機能:他の情報セキュリティエンティティの支援	情報セキュリティインシデントを適切に緩和し、また情報セキュリティインシデントから回復するために必要な管理および技術的活動を、コンスティチュエンシーが実行できるようにする。
H-2. 内部不正検知・再発防止支援	「内部不正検知・再発防止支援」サービスは、発見された内部不正行為の内容を分析し、ログから検知できないか検討し、可能な場合、検知ロジックとしての実装を実現する。	N/A		
I-1. 意識啓発	「意識啓発」サービスは、	9.1 サービス:啓	9.1.1 機能:調査および情報	セキュリティ態勢の改善とリスクの

	CDC に関わるあらゆる関係者の意識を高め、ビジネス資産を保護するための適切なツール、ベストプラクティス、ポリシー、リソースの活用促進を実現する。	発	集約	予防・緩和のために、コンスティチュエンシーに伝えられる情報を集約、照合して、優先順位を付ける。
			9.1.2 機能:報告書および啓発資料の作成	異なる対象者にリーチする、または特定のコンテンツを可能な限り最善の方法で配信することを目標とし、関連性があるものとして収集・調査した情報を使用して、異なるメディアで資料を作成する。
			9.1.3 機能:情報の普及	セキュリティプラクティスについての認識とプラクティスの実装を改善するために、セキュリティに関連する情報を普及させる。
			9.1.4 機能:アウトリーチ	CSIRT のミッションの遂行を支援する、またはミッションに関わる可能性のある専門家または組織との関係を構築および維持する。
I-2. 教育・トレーニング	「教育・トレーニング」サービスは、CDC が支援する組織関係者への、セキュリテ	6.4 サービス:緩和と回復	6.4.4 機能:他の情報セキュリティエンティティの支援	情報セキュリティインシデントを適切に緩和し、また情報セキュリティインシデントから回復するために必要

	ィ分野に特化したトレーニングを支援する。			な管理および技術的活動を、コンスティチュエンシーが実行できるようにする。
		9.2 サービス:トレーニングと教育	9.2.1 機能:知識、スキル、能力要件の収集	必要な KSA に関してコンスティチュエンシーのニーズを適切に評価、特定、文書化し、適切なトレーニングおよび教育資料を開発してスキルレベルを改善する。
			9.2.2 機能:教育およびトレーニング資料の開発	コンスティチュエンシーの KSA ニーズを基に、様々な対象にリーチする、または特定のコンテンツを配信する上で最善とされる配信方法に適した教育、指導、トレーニング資料を開発する。
			9.2.3 機能:コンテンツの配信	CSIRT が、様々な対象者とコンテンツの特性に基づいて、コンスティチュエンシーにコンテンツを最適に配信できるようになるコンテンツ配信のための正式なプロセスを開発する。
			9.2.4 機能:メンタリング	CSIRT スタッフ、コンスティチュエンシーまたは外部の信頼できるパートナーが、確立された関係を通じて経験豊富なスタッフから学ぶためのプ

				ログラムを開発する。
			9.2.5 機能:CSIRT スタッフの専門的能力開発	スタッフメンバーが適切な計画を立ててキャリア形成を成功させることができるよう支援する。
I-3. セキュリティコンサルティング	「セキュリティコンサルティング」サービスは、ビジネスにおけるさまざまな業務で、セキュリティに関連したコンサルティングを実現する。	9.4 サービス:技術およびポリシーに関するアドバイス	9.4.4 機能:技術アドバイス	効果的なインシデントハンドリング活動を可能にする一方で、コンスティチュエンシーがリスクと脅威をよりよく管理し、現在の運用とセキュリティのベストプラクティスを実装できるような技術的アドバイスを提供する。
I-4. セキュリティベンダー連携	「セキュリティベンダー連携」サービスは、購入したセキュリティ製品・サービスについて、その提供元と直接対話できる関係を築き、セキュリティの対応で見つかった不具合への対応要求や、改善に向けた前向きなフィードバックを実現する。	N/A		
I-5. セキュリティ関連団体との	「セキュリティ関連団体との連携」サービスは、外部の	7.4 サービス:脆弱性の調整	7.4.1 機能:脆弱性の通知・報告	その他の CVD プロセスの関係者に新しい脆弱性情報を最初に共有また

連携	コミュニティへの参加を通じて、積極的な情報交換を実現する。そこで得られた情報は、セキュリティ活動に反映させることができる。			は報告する。
			7.4.2 機能:脆弱性利害関係者の調整	協調的な脆弱性の公開(CVD)の取り組みに関与する様々な利害関係者および参加者の間で継続した調整と情報共有を行う。
		8.3 サービス:コミュニケーション	8.3.1 機能:組織内外とのコミュニケーション	現在の状況とそれがどのように変化しているかをコンスティチュエンシー(およびその他)に知らせる。
			8.3.4 機能:普及・統合・情報共有	情報を集め、標準化し、準備し、コンスティチュエンシーおよびそれ以外の人々と共有する。
			8.3.5 機能:情報共有の管理	情報の移転が成功し、使用可能であることを確実にする。
			8.3.6 機能: フィードバック	内部および外部の情報源から受信されるデータの品質、タイムリーさ、正確性および関連性を改善する。
I-6. 技術報告	「技術報告」サービスは、監	N/A		

	視運用の結果についての報告を実現する。このような活動はシステムや IT インフラのセキュリティレベルの可視化に役立つ。			
I-7. 幹部向けセキュリティ報告	幹部向けセキュリティ報告」サービスは、組織のセキュリティレベルや運用のパフォーマンスの指標を際立たせるため、幹部向けの定期的な報告や統計的な分析を実現する。	N/A		

2. FIRST CSIRT Services Framework version 2.1.0 への対応

FIRST CSIRT Services Framework version 2.1.0			X.1060	
サービス	機能	目的	サービス	概要
5.1 サービス:監視と検知	5.1.1 機能:ログとセンサーの管理	ログソースとセンサーを管理する。	G-1. セキュリティアーキテクチャ実装	「セキュリティアーキテクチャ実装」サービスは、CDC の戦略マネジメント（カテゴリーA）で設計したセキュリティアーキテクチャの実装を実現する。
			G-2. ネットワークセキュリティ製品基本運用	「ネットワークセキュリティ製品基本運用」サービスは、ファイアウォール、不正侵入検知システム/不正侵入防止システム(IDS/IPS)、WAF、プロキシなどのネットワーク装置の運用を実現する。
			G-4. エンドポイントセキュリティ製品基本運	「エンドポイントセキュリティ製品基本運用」サービスは、アンチウイルスソフトのようなエンドポイントでの対策製品の運用を実現する。
			G-6. クラウドセキュリティ製品基本運用	「クラウドセキュリティ製品基本運用」サービスは、クラウドで提供されるセキュリティサービスの運用を実現する。
	5.1.2 機能:検知ユースケース管	検知ユースケースのポートフォリオを、ライフサイクル全体を	F-1. 事後分析	「事後分析」サービスは、CDC 関係者の手順やツールの見直しや改善を実現する

	理	通して管理する。		ため、インシデントの解決法の詳述を実現する。
			G-3. ネットワークセキュリティ製品高度運用	「ネットワークセキュリティ製品高度運用」サービスは、IDS/IPS や WAF などの攻撃検知機能を持った製品において、製品ベンダーの検知シグネチャでは不十分な場合に、組織独自のカスタムシグネチャ作成を実現する。
			G-5. エンドポイントセキュリティ製品高度運用	「エンドポイントセキュリティ製品高度運用」サービスは、エンドポイント内の不審なプログラム挙動を検出し、レジストリの状態やプロセスの実行状況などを収集・分析するエンドポイント対策製品の運用を実現する、必要に応じて、独自に IOC(Indicators of Compromise)を定義し、エンドポイントでの検知を実現する。
			G-7. クラウドセキュリティ製品高度運用	「クラウドセキュリティ製品高度運用」サービスは、攻撃検知機能を持つクラウド上のセキュリティサービスに対して、組織独自のカスタムシグネチャ作成を実現する。ベンダーが提供するシグネチャでは不十分な場合に、そのカスタムシグネチャを適用する。

			G-10. 分析基盤高度運用	「分析基盤高度運用」サービスは、市販の SIEM では取得できないシステムログやパケットキャプチャデータを保持し、それらのデータやシステムに対して独自の分析アルゴリズムやロジックを開発し、より詳細で正確な分析を組織独自のシステムとして実現する。
	5.1.3 機能:コンテキストデータ管理	検知および強化のためのコンテキストデータソースを管理する。	G-3. ネットワークセキュリティ製品高度運用	「ネットワークセキュリティ製品高度運用」サービスは、IDS/IPS や WAF などの攻撃検知機能を持った製品において、製品ベンダーの検知シグネチャでは不十分な場合に、組織独自のカスタムシグネチャ作成を実現する。
			G-5. エンドポイントセキュリティ製品高度運用	「エンドポイントセキュリティ製品高度運用」サービスは、エンドポイント内の不審なプログラム挙動を検出し、レジストリの状態やプロセスの実行状況などを収集・分析するエンドポイント対策製品の運用を実現する、必要に応じて、独自に IOC(Indicators of Compromise)を定義し、エンドポイントでの検知を実現する。
			G-7. クラウドセキュリティ製品高度運	「クラウドセキュリティ製品高度運用」サービスは、攻撃検知機能を持つクラウ

			用	ド上のセキュリティサービスに対して、組織独自のカスタムシグネチャ作成を実現する。ベンダーが提供するシグネチャでは不十分な場合に、そのカスタムシグネチャを適用する。
			G-10. 分析基盤高度運用	「分析基盤高度運用」サービスは、市販の SIEM では取得できないシステムログやパケットキャプチャデータを保持し、それらのデータやシステムに対して独自の分析アルゴリズムやロジックを開発し、より詳細で正確な分析を組織独自のシステムとして実現する。
5.2 サービス:イベント分析	5.2.1 機能:関連付け	他の潜在的または進行中のセキュリティインシデントに直接関連するイベントを特定する。	B-1. リアルタイム監視	「リアルタイム監視」サービスは、ログやネットワークフローからシステムの状態や不審な動きを監視・分析し、インシデントやイベントに応じて必要な情報を収集し、トリアージを支援する。
	5.2.2 機能:適格性確認	真陽性の検知を特定、分類し、優先順位付けするために、検知された潜在的な情報セキュリティインシデントをトリアージして適格性を確認する。	B-1. リアルタイム監視	「リアルタイム監視」サービスは、ログやネットワークフローからシステムの状態や不審な動きを監視・分析し、インシデントやイベントに応じて必要な情報を収集し、トリアージを支援する。
6.1 サービス:情	6.1.1 機能:情報	コンスティチュエンシーまたは	D-1. インシデント	「インシデント報告受付」サービスは、運

報セキュリティインシデント報告の受付	セキュリティインシデント報告の受理	第三者から報告された、情報セキュリティインシデントに関する情報を受付または受理する。	報告受付	用における分析報告の受け付けを実現する。報告の受領は組織内部からだけではなく、外部の組織からの場合もある。
	6.1.2 機能:情報セキュリティインシデントのトリアージと処理	報告された情報セキュリティインシデントについて、初めにレビュー、分類、優先順位付け、および処理を行う。	D-2. インシデントハンドリング	「インシデントハンドリング」サービスは、受け付けたインシデントに対処し、D-3 から D-7 の活動の調整を実現する。
6.2 サービス:情報セキュリティインシデントの分析	6.2.1 機能:情報セキュリティインシデントのトリアージ(優先順位付けと分類)	情報セキュリティインシデントを分類し、優先順位を付け、初期評価を行う。	D-3. インシデント分類	「インシデント分類」サービスは、発生したインシデントとその原因の種別について共通理解を促すために、インシデントの分類を実現する。
	6.2.2 機能:情報収集	情報セキュリティインシデントおよびその一部とみなされるすべての情報セキュリティイベントに関連する情報を取得し、カタログを作成し、保存および追跡する。	D-3. インシデント分類	「インシデント分類」サービスは、発生したインシデントとその原因の種別について共通理解を促すために、インシデントの分類を実現する。
	6.2.3 機能:詳細分析の調整	インシデントに関するその他の技術分析を開始して追跡する。	D-3. インシデント分類	「インシデント分類」サービスは、発生したインシデントとその原因の種別について共通理解を促すために、インシデントの分類を実現する。
	6.2.4 機能:情報	インシデントの根本原因を特定	D-4. インシデント	「インシデント対応・封じ込め」サービス

	セキュリティインシデントの根本原因分析	するため、悪用された脆弱性が存在したり、悪用が成功したりするのを許してしまった状況(ユーザーの行動を含むが、それに限定されない)を特定する。	対応・封じ込め	は、インシデントがすべてのリソースに広がるなど、被害や影響が拡大する前の封じ込めを実現する。
	6.2.5 機能:クロスインシデント相関	利用可能なすべての情報を使って、コンテキストを最大限に理解し、それ以外の方法では認識されなかった、または対処できなかった相互関係を検知できるようにする。	F-1. 事後分析	「事後分析」サービスは、CDC 関係者の手順やツールの見直しや改善を実現するため、インシデントの解決法の詳述を実現する。
6.3 サービス:アーティファクトとフォレンジック痕跡の分析	6.3.1 機能: メディアまたはサーフェス分析	アーティファクトから収集された情報を、他のパブリックおよびプライベートのアーティファクトや署名リポジトリと比較する。	C-1. フォレンジック分析	「フォレンジック分析」サービスは、何が発生したのかの判断を促進するため、セキュリティ関連資産から収集された、あるいはイベントに関連したデジタル証跡の分析を実現する。
	6.3.2 機能:リバース・エンジニアリング	アーティファクトの完全な機能を、その実行環境に関係なく断定するために、アーティファクトの詳細な静的分析を行う。	C-2. 検体解析	「検体解析」サービスは、フォレンジックの過程で発見された、攻撃者によって設置されたマルウェア、プログラムやスクリプトの解析を実現する。
	6.3.3 機能:ランタイムまたは動的解析	アーティファクトの操作に関する洞察を提供する。	C-2. 検体解析	「検体解析」サービスは、フォレンジックの過程で発見された、攻撃者によって設置されたマルウェア、プログラムやスク

				リプトの解析を実現する。
	6.3.4 機能:比較分析	カタログ化されたアーティファクトのファミリー分析など、共通の機能または意図の特定に重点を置いた分析を行う。	C-3. 追及・追跡	「追及・追跡」サービスは、環境に対するあらゆる攻撃の発生源を追及・追跡を実現するもので、これはセキュリティインシデントの抑制や分析の重要な成功要因となる。内部と外部の両方の攻撃者を追及・追跡できる能力（例えば、サイバーアトリビューション）があれば将来の攻撃を事前に防ぐことができる。
6.4 サービス:緩和と回復	6.4.1 機能:対応計画の策定	影響を受けたシステムの完全性を回復し、影響を受けたデータ、システム、およびネットワークを劣化していない動作状態に戻し、元のセキュリティ問題が再び悪用されるコンテキストを再生することなく、影響を受けたサービスを完全な機能に復元する計画を定義して実施する。	D-4. インシデント対応・封じ込め	「インシデント対応・封じ込め」サービスは、インシデントがすべてのリソースに広がるなど、被害や影響が拡大する前の封じ込めを実現する。
	6.4.2 機能:一時的な対策と封じ込め	情報セキュリティインシデントがこれ以上拡大しない、すなわち、現在影響を受けているシステムやユーザー、ドメインに限定して、これ以上の損失(文書の	D-4. インシデント対応・封じ込め	「インシデント対応・封じ込め」サービスは、インシデントがすべてのリソースに広がるなど、被害や影響が拡大する前の封じ込めを実現する。

		漏えい、データベースまたはデータの変更等を含む)が発生することがないように保証する対策を実施する。		
	6.4.3 機能:システムの復旧	影響を受けたドメインやインフラストラクチャ、ネットワークの修復および、同様の活動の再発防止に必要な変更を行う。	D-5. インシデント復旧	「インシデント復旧」サービスは、対象となるシステムを通常状態へ回復することを支援する。
	6.4.4 機能:他の情報セキュリティエンティティの支援	情報セキュリティインシデントを適切に緩和し、また情報セキュリティインシデントから回復するために必要な管理および技術的活動を、コンスティチュエンシーが実行できるようにする。	D-5. インシデント復旧	「インシデント復旧」サービスは、対象となるシステムを通常状態へ回復することを支援する。
			H-1. 内部不正対応・分析支援	「内部不正対応・分析支援」サービスは、内部不正が発覚した場合に、セキュリティ活動で取得したログから行動内容を整理することで、組織的な対応を支援する。
6.5 サービス:情報セキュリティインシデントの調整	6.5.1 機能:コミュニケーション	利害関係者と効果的に連携し、必要とされる機密性を提供する、適切な複数のコミュニケーションチャネルを確立する。	D-6. インシデント通知	「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。

	6.5.2 機能:通知の配信	情報セキュリティインシデントの影響を受けるエンティティ、またはインシデントへの対応に貢献できるエンティティにアラートを送る。また、これらのエンティティに対して、それぞれの役割や、期待される可能性のある協力や支援について理解してもらうのに必要な情報を提供する。	D-6. インシデント通知	「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。
	6.5.3 機能:関連情報の配信	特定されたエンティティとのコミュニケーションを維持し、それらのエンティティが利用可能な洞察と教訓から利益を得たり、改善された対応を適用したり、新たなアドホックな措置を講じたりできるようにするために、利用可能な情報の適切な流れを提供する。	D-6. インシデント通知	「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。
	6.5.4 機能:活動の調整	すべてのコミュニケーションと活動の状況を追跡する。	D-2. インシデントハンドリング	「インシデントハンドリング」サービスは、受け付けたインシデントに対処し、D-3 から D-7 の活動の調整を実現する。
	6.5.5 機能:報告	次のステップに関するさらなる	D-7. インシデント	「インシデント対応報告」サービスは、対

		決定が、その時点で可能な最良の状況把握に基づくよう、事業内のすべての関係エンティティが、確実に現在の活動状況に関する情報を持っているようにする。	対応報告	応が完了したインシデントのレポートの完成と報告を実現する（対策の試みが長期化する場合は、CDC の戦略マネジメント（カテゴリーA）に引き継がれる）。インシデント対応中に CDC 関係者が現状報告を必要とする場合は、中間報告を行う。
	6.5.6 機能:メディアとのコミュニケーション	風評や誤解を招くような情報の流布を避けるために、進行中のイベントに関する正確で分かりやすい、事実に基づいた情報を提供できるように(公共の)メディアと連携する。	D-7. インシデント対応報告	「インシデント対応報告」サービスは、対応が完了したインシデントのレポートの完成と報告を実現する（対策の試みが長期化する場合は、CDC の戦略マネジメント（カテゴリーA）に引き継がれる）。インシデント対応中に CDC 関係者が現状報告を必要とする場合は、中間報告を行う。
6.6 サービス:危機管理支援	6.6.1 機能:コンスティチュエンシーへの情報配信	危機への対処を支援するために確立されたコミュニケーションリソースを提供する。	D-6. インシデント通知	「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。
	6.6.2 機能:情報セキュリティの状況報告	危機管理チームが、現在の情報セキュリティインシデントと既知の脆弱性の完全な概要を把握し、これを全体的な優先事項と	D-6. インシデント通知	「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。

		戦略の一部として検討できるようにする。		
	6.6.3 機能:戦略的意思決定の伝達	現在起きている情報セキュリティインシデントに対して危機が与える影響について、他のエンティティにタイムリーに情報提供する。	D-6. インシデント通知	「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。
7.1 サービス:脆弱性の発見・調査	7.1.1 機能:インシデント対応の脆弱性発見	セキュリティインシデントの一部として悪用された脆弱性を特定する。	D-6. インシデント通知	「インシデント通知」サービスは、インシデント対応チームやその他関連するグループに対して、インシデント発生の伝達を実現する。
			F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。
	7.1.2 機能:公的情報源による脆弱性の発見	公的情報源またはその他の第三者の情報源を参照して、新しい脆弱性について知る	F-3. 外部脅威情報の収集・評価	「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現する。
	7.1.3 機能:脆弱性調査	意図的な活動または調査の結果として、新しい脆弱性を発見または探索する。	E-3. 脆弱性診断	「脆弱性診断」サービスは、ネットワーク、システム、アプリケーションの脆弱性を特定し、その脆弱性がどのように悪用

				されるか判断するとともに、リスクをどのように軽減できるかの提案を実現する。
			E-5. ペネトレーションテスト	「ペネトレーションテスト」サービスは、攻撃者に悪用される可能性のあるセキュリティの脆弱性を明らかにし、考えられる侵害方法の炙り出しを実現する。(例：脅威ベースのペネトレーションテスト)。
			E-6. 高度サイバー攻撃耐性評価	高度サイバー攻撃(APT)に対抗するための「高度サイバー攻撃耐性評価」サービスは、標的型メール訓練やソーシャルエンジニアリングテストを実施しながら、標的型攻撃に対する組織耐性の計測を実現する。
			E-7. サイバー攻撃対応力評価	「サイバー攻撃対応力評価」サービスは、攻撃発生を想定したシナリオに基づき、セキュリティ対応が実際に発動され、インシデントを遅滞なく終息させることができるかどうかの確認を実現する（サイバー攻撃対応演習と呼ぶ)。
7.2 サービス:脆弱性報告の取得	7.2.1 機能:脆弱性報告の受理	コンスティチュエンシーまたは第三者から報告された脆弱性に関する情報を受付または受理す	F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）

		る。		の収集を実現する。
			F-3. 外部脅威情報の収集・評価	「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現する。
	7.2.2 機能:脆弱性報告のトリアージと処理	脆弱性報告の初期レビュー、分類、優先順位付け、および処理を行う。	F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。
			F-3. 外部脅威情報の収集・評価	「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現する。
7.3 サービス:脆弱性分析	7.3.1 機能:脆弱性のトリアージ(検証と分類)	脆弱性を分類し、優先順位を付け、初期評価を行う。	F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。
			F-3. 外部脅威情報の収集・評価	「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現す

				る。
	7.3.2 機能:脆弱性の根本原因分析	脆弱性の原因となった、またはその存在を顕在化する設計上または実装上の欠陥を理解する。	F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。
			F-3. 外部脅威情報の収集・評価	「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現する。
	7.3.3 機能:脆弱性対策開発	潜在的な脆弱性を修正(是正)するため、または脆弱性が悪用される影響を緩和(軽減)するために必要な手順を開発する。	F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。
			F-3. 外部脅威情報の収集・評価	「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現する。
			F-4. 脅威情報報告	「脅威情報報告」サービスは、内部と外部の脅威情報を取りまとめ、詳細も含めたドキュメント化を実現する。
			G-13. 新規セキュリ	「新規セキュリティツール検証」サービ

			ティツール検証	スは、セキュリティ活動において新たな対策が必要となった場合に、新規のセキュリティ資産の設計・導入を実現する。
7.4 サービス:脆弱性の調整	7.4.1 機能:脆弱性の通知・報告	その他の CVD プロセスの関係者に新しい脆弱性情報を最初に共有または報告する。	I-5. セキュリティ関連団体との連携	「セキュリティ関連団体との連携」サービスは、外部のコミュニティへの参加を通じて、積極的な情報交換を実現する。そこで得られた情報は、セキュリティ活動に反映させることができる。
	7.4.2 機能:脆弱性利害関係者の調整	協調的な脆弱性の公開(CVD)の取り組みに関与する様々な利害関係者および参加者の間で継続した調整と情報共有を行う。	I-5. セキュリティ関連団体との連携	「セキュリティ関連団体との連携」サービスは、外部のコミュニティへの参加を通じて、積極的な情報交換を実現する。そこで得られた情報は、セキュリティ活動に反映させることができる。
7.5 サービス:脆弱性の開示	7.5.1 機能:脆弱性開示ポリシーとインフラストラクチャの整備	CSIRT が脆弱性をハンドリングして開示する方法、および脆弱性を開示するために使用されるメカニズムについて、フレームワークを提供し、期待値を設定するポリシーを策定し、維持する。	A-3. ポリシーの企画立案	「ポリシーの企画立案」サービスは、具体的なセキュリティポリシーの定義や、ガイドラインの作成に関するすべての活動を支援する。
	7.5.2 機能:脆弱性の公表・連絡・周知	脆弱性を検知、修正、または緩和し、将来の脆弱性の不正利用を防止できるようにコンスティチ	F-5. 脅威情報の活用	「脅威情報の活用」サービスは、あらゆるカテゴリーのセキュリティ対応のために、脅威情報の編纂と発信を実現する。

		ュエンシー(または一般の人々)に情報を提供する。		
	7.5.3 機能:脆弱性開示後のフィードバック	脆弱性の開示または文書に関する、コンスティチュエンシーからの質問または報告を受領し、回答する。	F-5. 脅威情報の活用	「脅威情報の活用」サービスは、あらゆるカテゴリーのセキュリティ対応のために、脅威情報の編纂と発信を実現する。
7.6 サービス:脆弱性対応	7.6.1 機能:脆弱性の検知・スキャン	設置されたシステムに既知の脆弱性が存在するかどうかの調査に積極的に取り組む。	E-3. 脆弱性診断	「脆弱性診断」サービスは、ネットワーク、システム、アプリケーションの脆弱性を特定し、その脆弱性がどのように悪用されるか判断するとともに、リスクをどのように軽減できるかの提案を実現する。
	7.6.2 機能:脆弱性の修正	脆弱性が悪用されないようにするために脆弱性を修正または緩和する。通常は、ベンダーが提供するパッチまたはその他のソリューションをタイムリーに適用する。	E-4. パッチ管理	「パッチ管理」サービスは、情報技術(IT)サービスの可用性を維持しながら、必要なセキュリティパッチのインストールを支援する。
8.1 サービス:データ取得	8.1.1 機能:ポリシーの集約、抽出、ガイダンス	インフラで何が起きている（と考えられる）のか把握するためにコンスティチュエンシーおよびその資産が準拠すべきコンテキストを確立する。	A-3. ポリシーの企画立案	「ポリシーの企画立案」サービスは、具体的なセキュリティポリシーの定義や、ガイドラインの作成に関するすべての活動を支援する。

	8.1.2 機能:機能、役割、アクション、主要リスクへの資産のマッピング	既存の資産、コンスティチュエンシー、ベースラインおよび期待される活動の知識を提供することで、異常な状況の観察を特定する分析機能を支援する。	E-2. 資産棚卸	「資産棚卸」サービスは、CDC の所掌範囲となるビジネスインフラ全体を構成するシステム、アセット、アプリケーションの全数調査の情報管理を実現する。
	8.1.3 機能:収集	分析・解釈サービスや他の CSIRT サービスを支援するために情報を収集する。	F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。
			F-3. 外部脅威情報の収集・評価	「外部脅威情報の収集・評価」サービスは、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現する。
	8.1.4 機能:データ処理と準備	CSIRT 活動および分析サービスの要件をサポートできる、信頼性と一貫性のある最新のデータセットを確立する。	F-5. 脅威情報の活用	「脅威情報の活用」サービスは、あらゆるカテゴリーのセキュリティ対応のために、脅威情報の編纂と発信を実現する。
8.2 サービス:分析と統合	8.2.1 機能:予測と推定	現在の状況の特定または将来の状況の予測を目的として、データ取得中に収集された情報を分析する。	F-2. 内部脅威情報の収集・分析	「内部脅威情報の収集・分析」サービスは、リアルタイム分析やインシデント対応に関する情報（内部インテリジェンス）の収集を実現する。
			F-3. 外部脅威情報	「外部脅威情報の収集・評価」サービス

			の収集・評価	は、新たな脆弱性、攻撃の傾向、マルウェアの挙動、悪意のある IP アドレスやドメインの情報（外部情報）の収集を実現する。
	8.2.2 機能:イベント検知(アラートや探索を通じて)	コンスティチュエンシーの現在の状況の詳細を断定し、確認する。	B-1. リアルタイム監視	「リアルタイム監視」サービスは、ログやネットワークフローからシステムの状態や不審な動きを監視・分析し、インシデントやイベントに応じて必要な情報を収集し、トリアージを支援する。
	8.2.3 機能:情報セキュリティインシデントマネジメントの意思決定支援	被害を抑制し、将来のリスクを緩和する、あるいは新しく発生した弱点を特定するのに役立つかもしれない新しい見識をインシデント中に特定する。	D-2. インシデントハンドリング	「インシデントハンドリング」サービスは、受け付けたインシデントに対処し、D-3 から D-7 の活動の調整を実現する。
	8.2.4 機能:状況的影響	現在観察されている事象や今後観察されうる事象が状況図に与えると予想される潜在的影響を決定する。	D-2. インシデントハンドリング	「インシデントハンドリング」サービスは、受け付けたインシデントに対処し、D-3 から D-7 の活動の調整を実現する。
8.3 サービス:コミュニケーション	8.3.1 機能:組織内外とのコミュニケーション	現在の状況とそれがどのように変化しているかをコンスティチュエンシー(およびその他)に知らせる。	I-5. セキュリティ関連団体との連携	「セキュリティ関連団体との連携」サービスは、外部のコミュニティへの参加を通じて、積極的な情報交換を実現する。そこで得られた情報は、セキュリティ活動に反映させることができる。

	8.3.2 機能:報告と推奨事項	結果、アーティファクトまたは所見を作成し、分析中に発見または作成された重大な情報を、受取手が理解できる方法と形式で伝える。	F-4. 脅威情報報告	「脅威情報報告」サービスは、内部と外部の脅威情報を取りまとめ、詳細も含めたドキュメント化を実現する。
	8.3.3 機能:実装	状況の変化に対してさらなる準備や対応をするためにコミュニケーションに基づいてコンスティチュエンシーの環境を調整する。	G-1. セキュリティアーキテクチャ実装	「セキュリティアーキテクチャ実装」サービスは、CDC の戦略マネジメント（カテゴリーA）で設計したセキュリティアーキテクチャの実装を実現する。
			G-3. ネットワークセキュリティ製品高度運用	「ネットワークセキュリティ製品高度運用」サービスは、IDS/IPS や WAF などの攻撃検知機能を持った製品において、製品ベンダーの検知シグネチャでは不十分な場合に、組織独自のカスタムシグネチャ作成を実現する。
			G-5. エンドポイントセキュリティ製品高度運用	「エンドポイントセキュリティ製品高度運用」サービスは、エンドポイント内の不審なプログラム挙動を検出し、レジストリの状態やプロセスの実行状況などを収集・分析するエンドポイント対策製品の運用を実現する、必要に応じて、独自にIOC(Indicators of Compromise)を定義

				し、エンドポイントでの検知を実現する。
			G-7. クラウドセキュリティ製品高度運用	「クラウドセキュリティ製品高度運用」サービスは、攻撃検知機能を持つクラウド上のセキュリティサービスに対して、組織独自のカスタムシグネチャ作成を実現する。ベンダーが提供するシグネチャでは不十分な場合に、そのカスタムシグネチャを適用する。
	8.3.4 機能:普及・統合・情報共有	情報を集め、標準化し、準備し、コンスティチュエンシーおよびそれ以外の人々と共有する。	I-5. セキュリティ関連団体との連携	「セキュリティ関連団体との連携」サービスは、外部のコミュニティへの参加を通じて、積極的な情報交換を実現する。そこで得られた情報は、セキュリティ活動に反映させることができる。
	8.3.5 機能:情報共有の管理	情報の移転が成功し、使用可能であることを確実にする。	I-5. セキュリティ関連団体との連携	「セキュリティ関連団体との連携」サービスは、外部のコミュニティへの参加を通じて、積極的な情報交換を実現する。そこで得られた情報は、セキュリティ活動に反映させることができる。
	8.3.6 機能: フィードバック	内部および外部の情報源から受信されるデータの品質、タイムリーさ、正確性および関連性を改善する。	I-5. セキュリティ関連団体との連携	「セキュリティ関連団体との連携」サービスは、外部のコミュニティへの参加を通じて、積極的な情報交換を実現する。そこで得られた情報は、セキュリティ活動に反映させることができる。

9.1 サービス:啓発	9.1.1 機能:調査および情報集約	セキュリティ態勢の改善とリスクの予防・緩和のために、コンスティチュエンシーに伝えられる情報を集約、照合して、優先順位を付ける。	I-1. 意識啓発	「意識啓発」サービスは、CDC に関わるあらゆる関係者の意識を高め、ビジネス資産を保護するための適切なツール、ベストプラクティス、ポリシー、リソースの活用促進を実現する。
	9.1.2 機能:報告書および啓発資料の作成	異なる対象者にリーチする、または特定のコンテンツを可能な限り最善の方法で配信することを目標とし、関連性があるものとして収集・調査した情報を使用して、異なるメディアで資料を作成する。	I-1. 意識啓発	「意識啓発」サービスは、CDC に関わるあらゆる関係者の意識を高め、ビジネス資産を保護するための適切なツール、ベストプラクティス、ポリシー、リソースの活用促進を実現する。
	9.1.3 機能:情報の普及	セキュリティプラクティスについての認識とプラクティスの実装を改善するために、セキュリティに関連する情報を普及させる。	I-1. 意識啓発	「意識啓発」サービスは、CDC に関わるあらゆる関係者の意識を高め、ビジネス資産を保護するための適切なツール、ベストプラクティス、ポリシー、リソースの活用促進を実現する。
	9.1.4 機能:アウトリーチ	CSIRT のミッションの遂行を支援する、またはミッションに関わる可能性のある専門家または組織との関係を構築および維持する。	I-1. 意識啓発	「意識啓発」サービスは、CDC に関わるあらゆる関係者の意識を高め、ビジネス資産を保護するための適切なツール、ベストプラクティス、ポリシー、リソースの活用促進を実現する。
9.2 サービス:ト	9.2.1 機能:知識、	必要な KSA に関してコンステ	I-2. 教育・トレーニ	「教育・トレーニング」サービスは、CDC

レーニングと教育	スキル、能力要件の収集	ィチュエンシーのニーズを適切に評価、特定、文書化し、適切なトレーニングおよび教育資料を開発してスキルレベルを改善する。	ング	が支援する組織関係者への、セキュリティ分野に特化したトレーニングを支援する。
	9.2.2 機能:教育およびトレーニング資料の開発	コンスティチュエンシーの KSA ニーズを基に、様々な対象にリーチする、または特定のコンテンツを配信する上で最善とされる配信方法に適した教育、指導、トレーニング資料を開発する。	I-2. 教育・トレーニング	「教育・トレーニング」サービスは、CDC が支援する組織関係者への、セキュリティ分野に特化したトレーニングを支援する。
	9.2.3 機能:コンテンツの配信	CSIRT が、様々な対象者とコンテンツの特性に基づいて、コンスティチュエンシーにコンテンツを最適に配信できるようになるコンテンツ配信のための正式なプロセスを開発する。	I-2. 教育・トレーニング	「教育・トレーニング」サービスは、CDC が支援する組織関係者への、セキュリティ分野に特化したトレーニングを支援する。
	9.2.4 機能:メンタリング	CSIRT スタッフ、コンスティチュエンシーまたは外部の信頼できるパートナーが、確立された関係を通じて経験豊富なスタッフから学ぶためのプログラムを開発する。	I-2. 教育・トレーニング	「教育・トレーニング」サービスは、CDC が支援する組織関係者への、セキュリティ分野に特化したトレーニングを支援する。

	9.2.5 機能:CSIRT スタッフの専門的能力開発	スタッフメンバーが適切な計画を立ててキャリア形成を成功させることができるよう支援する。	I-2. 教育・トレーニング	「教育・トレーニング」サービスは、CDCが支援する組織関係者への、セキュリティ分野に特化したトレーニングを支援する。
9.3 サービス:演習	9.3.1 機能:要件分析	演習の、あらかじめ決められた範囲と焦点の特定の課題に集中することにより、確実に十分な成果を得られるようにする。	E-6. 高度サイバー攻撃耐性評価	高度サイバー攻撃(APT)に対抗するための「高度サイバー攻撃耐性評価」サービスは、標的型メール訓練やソーシャルエンジニアリングテストを実施しながら、標的型攻撃に対する組織耐性の計測を実現する。
			E-7. サイバー攻撃対応力評価	「サイバー攻撃対応力評価」サービスは、攻撃発生を想定したシナリオに基づき、セキュリティ対応が実際に発動され、インシデントを遅滞なく終息させることができるかどうかの確認を実現する（サイバー攻撃対応演習と呼ぶ)。
	9.3.2 機能:フォーマットと環境の開発	演習の実施に必要な内部および外部のリソースとインフラストラクチャを特定および決定する。	E-6. 高度サイバー攻撃耐性評価	高度サイバー攻撃(APT)に対抗するための「高度サイバー攻撃耐性評価」サービスは、標的型メール訓練やソーシャルエンジニアリングテストを実施しながら、標的型攻撃に対する組織耐性の計測を実現する。
			E-7. サイバー攻撃	「サイバー攻撃対応力評価」サービスは、

			対応力評価	攻撃発生を想定したシナリオに基づき、セキュリティ対応が実際に発動され、インシデントを遅滞なく終息させることができるかどうかの確認を実現する（サイバー攻撃対応演習と呼ぶ)。
	9.3.3 機能:シナリオ開発	コミュニケーションの観点を含む、模擬サイバーセキュリティイベントやインシデントのハンドリングを通して、そのサービスと機能の効率と有効性、およびそのスキル、知識、能力を改善する機会を対象者に提供する。	E-6. 高度サイバー攻撃耐性評価	高度サイバー攻撃(APT)に対抗するための「高度サイバー攻撃耐性評価」サービスは、標的型メール訓練やソーシャルエンジニアリングテストを実施しながら、標的型攻撃に対する組織耐性の計測を実現する。
			E-7. サイバー攻撃対応力評価	「サイバー攻撃対応力評価」サービスは、攻撃発生を想定したシナリオに基づき、セキュリティ対応が実際に発動され、インシデントを遅滞なく終息させることができるかどうかの確認を実現する（サイバー攻撃対応演習と呼ぶ)。
	9.3.4 機能:演習の実行	CSIRT チームが組織の CSIRT 計画の妥当性とその実行能力に対する信頼を高めるためにドリル・演習を実施する。	E-6. 高度サイバー攻撃耐性評価	高度サイバー攻撃(APT)に対抗するための「高度サイバー攻撃耐性評価」サービスは、標的型メール訓練やソーシャルエンジニアリングテストを実施しながら、標的型攻撃に対する組織耐性の計測を実現

				する。
			E-7. サイバー攻撃対応力評価	「サイバー攻撃対応力評価」サービスは、攻撃発生を想定したシナリオに基づき、セキュリティ対応が実際に発動され、インシデントを遅滞なく終息させることができるかどうかの確認を実現する（サイバー攻撃対応演習と呼ぶ)。
	9.3.5 機能:演習成果レビュー	実際の観察に基づいて、演習の形式的で客観的な分析を行う。	E-6. 高度サイバー攻撃耐性評価	高度サイバー攻撃(APT)に対抗するための「高度サイバー攻撃耐性評価」サービスは、標的型メール訓練やソーシャルエンジニアリングテストを実施しながら、標的型攻撃に対する組織耐性の計測を実現する。
			E-7. サイバー攻撃対応力評価	「サイバー攻撃対応力評価」サービスは、攻撃発生を想定したシナリオに基づき、セキュリティ対応が実際に発動され、インシデントを遅滞なく終息させることができるかどうかの確認を実現する（サイバー攻撃対応演習と呼ぶ)。
9.4 サービス:技術およびポリシーに関するアドバイス	9.4.1 機能:リスクマネジメント支援	情報セキュリティおよびその他の関連機能と連携して、機会と脅威の特定能力を改善し、統制・管理を改善し、損失防止および	A-2. リスクアセスメント	「リスクアセスメント」サービスは、組織の資産や脅威、セキュリティ対策の観点から、組織のリスクレベル把握を実現する。

		インシデントマネジメントを改善する。		
	9.4.2 機能:事業継続および災害復旧計画の支援	事業継続と災害復旧に関する信頼されるアドバイザーとして、中立的で事実に基づいたアドバイスを提供し、そのアドバイスを使用できる環境と適用されるリソースの制約を考慮する。	A-5. 事業継続性	「事業継続性」サービスは、組織の事業継続計画の実現や実行が正しく行われるために必要な経営上の機能を支援する。
	9.4.3 機能:ポリシーの支援	アドバイスが利用される可能性のある環境および適用されるリソースの制約を考慮し、公平で事実に基づいたアドバイスを提供することにより、ポリシーの開発および実施について信頼されるアドバイザーとして行動する。	A-3. ポリシーの企画立案	「ポリシーの企画立案」サービスは、具体的なセキュリティポリシーの定義や、ガイドラインの作成に関するすべての活動を支援する。
	9.4.4 機能:技術アドバイス	効果的なインシデントハンドリング活動を可能にする一方で、コンスティチュエンシーがリスクと脅威をよりよく管理し、現在の運用とセキュリティのベストプラクティスを実装できるような技術的アドバイスを提供す	I-3. セキュリティコンサルティング	「セキュリティコンサルティング」サービスは、ビジネスにおけるさまざまな業務で、セキュリティに関連したコンサルティングを実現する。

		る。		
N/A			A-1. リスクマネジメント	「リスクマネジメント」サービスは、リスクに対して組織を方向づけ、コントロールできるよう、A-2 から A-13 を含む統括的な活動を実現する。
N/A			A-4. ポリシー管理	「ポリシー管理」サービスは、ポリシーや組織の規定を評価して定期的に見直しや、新たな外部要件（例えば、規制やガイドライン）への準拠を実現する。
N/A			A-6. 事業影響度分析	「事業影響度分析」のサービスは、様々なイベントやシナリオから起こり得る影響の体系的なアセスメントを実現する。このサービスは、発生しうる損失の規模を組織が理解するのに役立つ。直接的な金銭的損失だけでなく、利害関係者の信頼喪失や風評被害など、その他の影響も対象となる場合もある。
N/A			A-7. リソース管理	「リソース管理」サービスは、各種セキュリティ活動を支えるリソース（人、予算、システムなど）計画と、各サービスへの適切な割り当てを実現する。
N/A			A-8. セキュリティアーキテクチャ設計	「セキュリティアーキテクチャ設計」サービスは、ビジネスをセキュアにするた

				めのアーキテクチャの確立を実現する。システムの設計やビジネスプロセスの制約（例えば、 サプライチェーン）を考慮した各種セキュリティ対策をまとめ、CDC のプラットフォーム（カテゴリーGにあるような）の開発や維持を実現する。
N/A			A-9. トリアージ基準管理	「トリアージ基準管理」サービスは、全社のポリシーで合意された範囲内で発覚した事象（例えば、インシデント、脆弱性の発覚、脅威情報の発見など）へのトリアージ（対応の優先順位）基準作成を実現する。
N/A			A-10. 対応策選定	「対応策選定」サービスは、A-9 のトリアージ基準に対する対応策や、各種のセキュリティ対策に最も適切な技術の選定活動を支援する。
N/A			A-11. 品質管理	「品質管理」サービスは、セキュリティ活動の品質に問題がないかどうか、ビジネスに悪影響を与えていないかどうか（ユーザビリティ、生産性など）の一定期間（1週間、1 ヶ月など）ごとの点検を実施する。
N/A			A-12. セキュリティ	「セキュリティ監査」サービスは、組織が

			監査	特定の拠点や期間において、セキュリティポリシーや統制をどのように実現しているかの体系的かつ定量的な監査を実現する。CDC 関係者は、必要な情報の統制の実施状況の証拠を提供するために、監査活動に間接的に関与する。
N/A			A-13. 認証	「認証」サービスは、組織がさまざまな規格や認証スキームの適合に向けた活動を支援する。
N/A			B-2. イベントデータ保管	「イベントデータ保管」サービスは、セキュリティ監視や分析で収集されたイベントを集約し、一元的な保管を実現する。
N/A			B-3. 通知・警告	「通知・警告」サービスは、情報資産に対する潜在的なリスクがハイライトされたイベント（セキュリティ機器の警告、セキュリティ速報、脆弱性、拡散する脅威など）を、関係する内部で役目を持ったものへの通知を実現する。
N/A			B-4. レポート問い合わせ対応	「レポート問い合わせ対応」サービスは、分析に関するデータやレポートに関する問い合わせ対応を実現する。
N/A			C-4. 証拠収集	「証拠収集」サービスは、扱われたインシデントに関係する電磁的証拠を収集・保

				全し、証拠としての妥当性の維持を実現する（証拠保全の一貫性）。
N/A			E-1. ネットワーク情報収集	「ネットワーク情報収集」サービスは、保護対象となるネットワーク構成の概要の収集を実現する。
N/A			E-8. ポリシー遵守	「ポリシー遵守」サービスは、事前に定義されたセキュリティポリシーへの適合性と遵守の検証を支援する。
N/A			E-9. 堅牢化	「堅牢化」サービスは、システムに対するセキュリティ設定の見極めや評価、適用するため、および攻撃のリスクの低減や排除のための、IT コンポーネントの構成最適化を実現する。
N/A			G-8. 深掘分析ツール運用	「深堀分析ツール運用」サービスは、デジタルフォレンジックや、マルウェア解析のような深堀分析に用いるツールの運用を実現する。
N/A			G-9. 分析基盤基本運用	「分析基盤基本運用」サービスは、必要なログデータを蓄積し、日常的に、主にはリアルタイム分析を行うことができるSIEM(Security Information and Event Management)のような分析基盤の運用を実現する。

N/A			G-11. CDC システム運用	「CDC システム運用」サービスは、これまでに記した各種セキュリティ対応ツール、各種レポート作成、問い合わせ対応、脆弱性管理システムなど、セキュリティ対応業務に必要なタスクを遂行するシステムの運用を実現する。
N/A			G-12. 既設セキュリティツール検証	「既設セキュリティツール検証」サービスは、既に存在するセキュリティ対応ツールのバージョンアップや設定変更時の、システムや運用への主に可用性の観点での影響検証を実現する。
N/A			H-2. 内部不正検知・再発防止支援	「内部不正検知・再発防止支援」サービスは、発見された内部不正行為の内容を分析し、ログから検知できないか検討し、可能な場合、検知ロジックとしての実装を実現する。
N/A			I-4. セキュリティベンダー連携	「セキュリティベンダー連携」サービスは、購入したセキュリティ製品・サービスについて、その提供元と直接対話できる関係を築き、セキュリティの対応で見つかった不具合への対応要求や、改善に向けた前向きなフィードバックを実現する。

N/A			I-6. 技術報告	「技術報告」サービスは、監視運用の結果についての報告を実現する。このような活動はシステムや IT インフラのセキュリティレベルの可視化に役立つ。
N/A			I-7. 幹部向けセキュリティ報告	幹部向けセキュリティ報告」サービスは、組織のセキュリティレベルや運用のパフォーマンスの指標を際立たせるため、幹部向けの定期的な報告や統計的な分析を実現する。

執筆

日本セキュリティオペレーション事業者協議会（ISOG-J）

セキュリティオペレーション連携 WG(WG6)

武井 滋紀　　SCSK セキュリティ株式会社

/　ISOG-J WG6 リーダー

河島 君知　　NTT データ先端技術株式会社

後藤 秀斗　　NTT データ先端技術株式会社

執筆協力

中村 裕太　　NTT テクノクロス株式会社

（執筆関係者、社名五十音順）