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)

© 2025 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) isogj.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
2.	FIRST CSIRT Services Framework version 2.1.0 への対応

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

X.1060		FIRST CSIRT Ser	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	「リスクマネジメント」サ	N/A			
ジメント	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。				
A-2. リスクアセ	「リスクアセスメント」サ	9.4 サービス:技	9.4.1 機能:リスクマネジメ	情報セキュリティおよびその他の関	
スメント	ービスは、組織の資産や脅	術およびポリシ	ント支援	連機能と連携して、機会と脅威の特定	
	威、セキュリティ対策の観	ーに関するアド		能力を改善し、統制・管理を改善し、	
	点から、組織のリスクレベ	バイス		損失防止およびインシデントマネジ	
	ル把握を実現する。			メントを改善する。	
A-3. ポリシーの	「ポリシーの企画立案」サ	7.5 サービス:脆	7.5.1 機能:脆弱性開示ポリ	CSIRT が脆弱性をハンドリングして	
企画立案	ービスは、具体的なセキュ	弱性の開示	シーとインフラストラクチ	開示する方法、および脆弱性を開示す	
	リティポリシーの定義や、		ャの整備	るために使用されるメカニズムにつ	
	ガイドラインの作成に関す			いて、フレームワークを提供し、期待	
	るすべての活動を支援す			値を設定するポリシーを策定し、維持	
	る。			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	

		5 T /B	H. II. 18 232) a) a) [m[m]] a) b)
		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	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
		術およびポリシ		る環境および適用されるリソースの
		ーに関するアド		制約を考慮し、公平で事実に基づいた
		バイス		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	「ポリシー管理」サービス	N/A		
理	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。			
A-5. 事業継続性	「事業継続性」サービスは、	9.4 サービス:技	9.4.2 機能:事業継続および	事業継続と災害復旧に関する信頼さ
	組織の事業継続計画の実現	術およびポリシ	災害復旧計画の支援	れるアドバイザーとして、中立的で事
	や実行が正しく行われるた	ーに関するアド		実に基づいたアドバイスを提供し、そ
	めに必要な経営上の機能を	バイス		のアドバイスを使用できる環境と適
	支援する。			用されるリソースの制約を考慮する。
A-6. 事業影響度	「事業影響度分析」のサー	N/A		
分析	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。			
「リソース管理」サービス	N/A		
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。			
「セキュリティアーキテク	N/A		
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			
	響を実現する。このは、このでででは、というでは、というでででででででででででででででででででででででででででででででででででで	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。 「リソース管理」サービスは、予算、システムなど)計画と、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。 「セキュリティ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	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。 「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。 「セキュリティ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

	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	「トリアージ基準管理」サ	N/A	
基準管理	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。		
A-10. 対応策選	「対応策選定」サービスは、	N/A	
定	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。		
A-11. 品質管理	「品質管理」サービスは、セ	N/A	
	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。			
A-12. セキュリ		N/A		
ティ監査	ビスは、組織が特定の拠点	17/11		
/ 1 <u>III. H.</u>	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。			
A-13. 認証	「認証」サービスは、組織が	N/A		
	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。			
B-1. リアルタイ	「リアルタイム監視」サー	5.2 サービス:イ	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
ム監視	ビスは、ログやネットワー	ベント分析		ティインシデントに直接関連するイ
	クフローからシステムの状			ベントを特定する。
	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。
		8.2 サービス:分	8.2.2 機能:イベント検知(ア	コンスティチュエンシーの現在の状
		析と統合	ラートや探索を通じて)	況の詳細を断定し、確認する。
B-2. イベントデ	「イベントデータ保管」サ	N/A		
ータ保管	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。			
B-3. 通知・警告	「通知・警告」サービスは、	N/A		
	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。			
B-4. レポート問	「レポート問い合わせ対	N/A		
い合わせ対応	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。			
C-1. フォレンジ	「フォレンジック分析」サ	6.3 サービス:ア	6.3.1 機能: メディアまたは	アーティファクトから収集された情
ック分析	ービスは、何が発生したの	ーティファクト	サーフェス分析	報を、他のパブリックおよびプライベ
	かの判断を促進するため、	とフォレンジッ		ートのアーティファクトや署名リポ
	セキュリティ関連資産から	ク痕跡の分析		ジトリと比較する。
	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。			
C-2. 検体解析	「検体解析」サービスは、フ	6.3 サービス:ア	6.3.2 機能:リバース・エンジ	アーティファクトの完全な機能を、そ
	ォレンジックの過程で発見	ーティファクト	ニアリング	の実行環境に関係なく断定するため
	された、攻撃者によって設	とフォレンジッ		に、アーティファクトの詳細な静的分
	置されたマルウェア、プロ	ク痕跡の分析		析を行う。
	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	アーティファクトの操作に関する洞
			は動的解析	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	ーティファクト		のファミリー分析など、共通の機能ま
	の発生源を追及・追跡を実	とフォレンジッ		たは意図の特定に重点を置いた分析
	現するもので、これはセキ	ク痕跡の分析		を行う。
	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。			
C-4. 証拠収集	「証拠収集」サービスは、扱	N/A		
	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)。			
D-1. インシデン	「インシデント報告受付」	6.1 サービス:情	6.1.1 機能:情報セキュリテ	コンスティチュエンシーまたは第三
卜報告受付	サービスは、運用における	報セキュリティ	ィインシデント報告の受理	者から報告された、情報セキュリティ
	分析報告の受け付けを実現	インシデント報		インシデントに関する情報を受付ま
	する。報告の受領は組織内	告の受付		たは受理する。
	部からだけではなく、外部			
	の組織からの場合もある。			

		1		
D-2. インシデン	「インシデントハンドリン	6.1 サービス:情	6.1.2 機能:情報セキュリテ	報告された情報セキュリティインシ
トハンドリング	グ」サービスは、受け付けた	報セキュリティ	ィインシデントのトリアー	デントについて、初めにレビュー、分
	インシデントに対処し、D-3	インシデント報	ジと処理	類、優先順位付け、および処理を行う。
	から D-7 の活動の調整を実	告の受付		
	現する。			
		6.5 サービス:情	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
		報セキュリティ		の状況を追跡する。
		インシデントの		
		調整		
		8.2 サービス:分	8.2.3 機能:情報セキュリテ	被害を抑制し、将来のリスクを緩和す
		析と統合	ィインシデントマネジメン	る、あるいは新しく発生した弱点を特
			トの意思決定支援	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	「インシデント分類」サー	6.2 サービス:情	6.2.1 機能:情報セキュリテ	情報セキュリティインシデントを分
ト分類	ビスは、発生したインシデ	報セキュリティ	ィインシデントのトリアー	類し、優先順位を付け、初期評価を行
	ントとその原因の種別につ	インシデントの	ジ(優先順位付けと分類)	う。
	いて共通理解を促すため	分析		
	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。
			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	「インシデント対応・封じ	6.2 サービス:情	6.2.4 機能:情報セキュリテ	インシデントの根本原因を特定する
ト対応・封じ込め	込め」サービスは、インシデ	報セキュリティ	ィインシデントの根本原因	ため、悪用された脆弱性が存在した
	ントがすべてのリソースに	インシデントの	分析	り、悪用が成功したりするのを許して
	広がるなど、被害や影響が	分析		しまった状況(ユーザーの行動を含む
	拡大する前の封じ込めを実			が、それに限定されない)を特定する。
	現する。			
		6.4 サービス:緩	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
		和と回復		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	情報セキュリティインシデントがこ
			封じ込め	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	「インシデント復旧」サー	6.4 サービス:緩	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
卜復旧	ビスは、対象となるシステ	和と回復		トラクチャ、ネットワークの修復およ
	ムを通常状態へ回復するこ			び、同様の活動の再発防止に必要な変
	とを支援する。			更を行う。
			6.4.4 機能:他の情報セキュ	情報セキュリティインシデントを適
			リティエンティティの支援	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	「インシデント通知」サー	6.5 サービス:情	6.5.1 機能:コミュニケーシ	利害関係者と効果的に連携し、必要と
卜通知	ビスは、インシデント対応	報セキュリティ	ョン	される機密性を提供する、適切な複数
	チームやその他関連するグ	インシデントの		のコミュニケーションチャネルを確
	ループに対して、インシデ	調整		立する。
	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。
		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	6.6.1 機能:コンスティチュ	危機への対処を支援するために確立
	機管理支援	エンシーへの情報配信	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	危機管理チームが、現在の情報セキュ
		ィの状況報告	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	7.1.1 機能:インシデント対	セキュリティインシデントの一部と
		弱性の発見・調査	応の脆弱性発見	して悪用された脆弱性を特定する。
D-7. インシデン	「インシデント対応報告」	6.5 サービス:情	6.5.5 機能:報告	次のステップに関するさらなる決定
ト対応報告	サービスは、対応が完了し	報セキュリティ		が、その時点で可能な最良の状況把握
	たインシデントのレポート	インシデントの		に基づくよう、事業内のすべての関係
	の完成と報告を実現する	調整		エンティティが、確実に現在の活動状
	(対策の試みが長期化する			況に関する情報を持っているように
	場合は、CDC の戦略マネジ			する。
	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	風評や誤解を招くような情報の流布
			ミュニケーション	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	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
		ミュニケーショ		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	「ネットワーク情報収集」	N/A		
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。			
E-2. 資産棚卸	「資産棚卸」サービスは、	8.1 サービス:デ	8.1.2 機能:機能、役割、アク	既存の資産、コンスティチュエンシ
	CDC の所掌範囲となるビ	ータ取得	ション、主要リスクへの資産	ー、ベースラインおよび期待される活
	ジネスインフラ全体を構成		のマッピング	動の知識を提供することで、異常な状
	するシステム、アセット、ア			況の観察を特定する分析機能を支援
	プリケーションの全数調査			する。
	の情報管理を実現する。			
E-3. 脆弱性診断	「脆弱性診断」サービスは、	7.1 サービス:脆	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
	ネットワーク、システム、ア	弱性の発見・調査		て、新しい脆弱性を発見または探索す
	プリケーションの脆弱性を			る。
	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 サービス:脆	7.6.1 機能:脆弱性の検知・ス	設置されたシステムに既知の脆弱性
		弱性対応	キャン	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、	76 サービス: 脆	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
	情報技術(IT)サービスの可	弱性対応		めに脆弱性を修正または緩和する。通
	用性を維持しながら、必要	99 1工7/1//0		常は、ベンダーが提供するパッチまた
	なセキュリティパッチのイ			はその他のソリューションをタイム
	ンストールを支援する。			リーに適用する。
DF °>11		日の 山 18 つ・時	見ら 1 機分・脱去記はの投票 フ	
E-5. ペネトレー	「ペネトレーションテス		7.6.1 機能:脆弱性の検知・ス	設置されたシステムに既知の脆弱性
ションテスト	ト」サービスは、攻撃者に悪	弱性対応	キャン	が存在するかどうかの調査に積極的
	用される可能性のあるセキ			に取り組む。
	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	高度サイバー攻撃(APT)に	9.3 サービス:演	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
一攻擊耐性評価	対抗するための「高度サイ	習		焦点の特定の課題に集中することに
	バー攻撃耐性評価」サービ			より、確実に十分な成果を得られるよ
	スは、標的型メール訓練や			うにする。
	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。			
			099機能・フェーラート	冷羽の字特に以面も内切むとだり切
			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	実際の観察に基づいて、演習の形式的
			<u> </u>	で客観的な分析を行う。
E-7. サイバー攻	「サイバー攻撃対応力評	9.3 サービス:演	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
擊対応力評価	価」サービスは、攻撃発生を	習		焦点の特定の課題に集中することに
	想定したシナリオに基づ			より、確実に十分な成果を得られるよ
	き、セキュリティ対応が実			うにする。
	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	演習の実施に必要な内部および外部

			.m. r.t	
			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	実際の観察に基づいて、演習の形式的
			<u> </u>	で客観的な分析を行う。
E-8. ポリシー遵	「ポリシー遵守」サービス	N/A		
守	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。			
E-9. 堅牢化	「堅牢化」サービスは、シス	N/A		
	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。			
F-1. 事後分析	「事後分析」サービスは、	5.1 サービス:監	5.1.2 機能:検知ユースケー	検知ユースケースのポートフォリオ
	CDC 関係者の手順やツー	視と検知	ス管理	を、ライフサイクル全体を通して管理
	ルの見直しや改善を実現す			する。
	るため、インシデントの解			
	決法の詳述を実現する。			
		6.2 サービス:情	6.2.5 機能:クロスインシデ	利用可能なすべての情報を使って、コ
		報セキュリティ	ント相関	ンテキストを最大限に理解し、それ以
		インシデントの		外の方法では認識されなかった、また
		分析		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	「内部脅威情報の収集・分	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
報の収集・分析	析」サービスは、リアルタイ	ーティファクト		のファミリー分析など、共通の機能ま
	ム分析やインシデント対応	とフォレンジッ		たは意図の特定に重点を置いた分析
	に関する情報(内部インテ	ク痕跡の分析		を行う。
	リジェンス) の収集を実現			
	する。			
		7.1 サービス:脆	7.1.1 機能:インシデント対	セキュリティインシデントの一部と
		弱性の発見・調査	応の脆弱性発見	して悪用された脆弱性を特定する。
		7.2 サービス:脆	7.2.1 機能:脆弱性報告の受	コンスティチュエンシーまたは第三
		弱性報告の取得	理	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	脆弱性報告の初期レビュー、分類、優
			リアージと処理	先順位付け、および処理を行う。
		7.3 サービス:脆	7.3.1 機能:脆弱性のトリア	脆弱性を分類し、優先順位を付け、初
		弱性分析	ージ(検証と分類)	期評価を行う。
			7.3.2 機能:脆弱性の根本原	脆弱性の原因となった、またはその存
			因分析	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	8.1.3 機能:収集	分析・解釈サービスや他の CSIRT サ
		ータ取得		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	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
		析と統合		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	「外部脅威情報の収集・評	7.1 サービス:脆	7.1.2 機能:公的情報源によ	公的情報源またはその他の第三者の
報の収集・評価	価」サービスは、新たな脆弱	弱性の発見・調査	る脆弱性の発見	情報源を参照して、新しい脆弱性につ
	性、攻撃の傾向、マルウェア			いて知る
	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 サービス:脆	7.2.1 機能:脆弱性報告の受	コンスティチュエンシーまたは第三
		弱性報告の取得	理	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	脆弱性報告の初期レビュー、分類、優
			リアージと処理	先順位付け、および処理を行う。
		7.3 サービス:脆	7.3.1 機能:脆弱性のトリア	脆弱性を分類し、優先順位を付け、初
		弱性分析	ージ(検証と分類)	期評価を行う。
			7.3.2 機能:脆弱性の根本原	脆弱性の原因となった、またはその存
			因分析	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	8.1.3 機能:収集	分析・解釈サービスや他の CSIRT サ
		ータ取得		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	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
		析と統合		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	「脅威情報報告」サービス	7.3 サービス:脆	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
告	は、内部と外部の脅威情報	弱性分析		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			緩和(軽減)するために必要な手順を開
	たドキュメント化を実現す			発する。
	る。			
		8.3 サービス:コ	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
		ミュニケーショ		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。
F-5. 脅威情報の	「脅威情報の活用」サービ	7.5 サービス:脆	7.5.2 機能:脆弱性の公表・連	脆弱性を検知、修正、または緩和し、
活用	スは、あらゆるカテゴリー	弱性の開示	絡・周知	将来の脆弱性の不正利用を防止でき
	のセキュリティ対応のため			るようにコンスティチュエンシー(ま
	に、脅威情報の編纂と発信			たは一般の人々)に情報を提供する。
	を実現する。			
			7.5.3 機能:脆弱性開示後の	脆弱性の開示または文書に関する、コ
			フィードバック	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	8.1.4 機能:データ処理と準	CSIRT 活動および分析サービスの要
		ータ取得	備	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	「セキュリティアーキテク	5.1 サービス:監	5.1.1 機能:ログとセンサー	ログソースとセンサーを管理する。
ィアーキテクチ	チャ実装」サービスは、CDC	視と検知	の管理	
ャ実装	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。			
		8.3 サービス:コ	8.3.3 機能:実装	状況の変化に対してさらなる準備や
		ミュニケーショ		対応をするためにコミュニケーショ
		ン		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	「ネットワークセキュリテ	5.1 サービス:監	5.1.1 機能:ログとセンサー	ログソースとセンサーを管理する。
クセキュリティ	ィ製品基本運用」サービス	視と検知	の管理	
製品基本運用	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-3. ネットワー	「ネットワークセキュリテ	5.1 サービス:監	5.1.2 機能:検知ユースケー	検知ユースケースのポートフォリオ
クセキュリティ	ィ製品高度運用」サービス	視と検知	ス管理	を、ライフサイクル全体を通して管理
製品高度運用	は、IDS/IPS やWAF など			する。
	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。			

		I	T	
			5.1.3 機能:コンテキストデ	検知および強化のためのコンテキス
			ータ管理	トデータソースを管理する。
		8.3 サービス:コ	8.3.3 機能:実装	状況の変化に対してさらなる準備や
		ミュニケーショ		対応をするためにコミュニケーショ
		ン		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	「エンドポイントセキュリ	5.1 サービス:監	5.1.1 機能:ログとセンサー	ログソースとセンサーを管理する。
ントセキュリテ	ティ製品基本運用」サービ	視と検知	の管理	
ィ製品基本運	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-5. エンドポイ	「エンドポイントセキュリ	5.1 サービス:監	5.1.2 機能:検知ユースケー	検知ユースケースのポートフォリオ
ントセキュリテ	ティ製品高度運用」サービ	視と検知	ス管理	を、ライフサイクル全体を通して管理
ィ製品高度運用	スは、エンドポイント内の			する。
	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。			
			5.1.3 機能:コンテキストデ	検知および強化のためのコンテキス
			ータ管理	トデータソースを管理する。
		8.3 サービス:コ	8.3.3 機能:実装	状況の変化に対してさらなる準備や
		ミュニケーショ		対応をするためにコミュニケーショ
		ン		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	「クラウドセキュリティ製	5.1 サービス:監	5.1.1 機能:ログとセンサー	ログソースとセンサーを管理する。
キュリティ製品	品基本運用」サービスは、ク	視と検知	の管理	
基本運用	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。			
G-7. クラウドセ	「クラウドセキュリティ製	5.1 サービス:監	5.1.2 機能:検知ユースケー	検知ユースケースのポートフォリオ
キュリティ製品	品高度運用」サービスは、攻	視と検知	ス管理	を、ライフサイクル全体を通して管理
高度運用	撃検知機能を持つクラウド			する。
	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。			

			5.1.3 機能:コンテキストデ	検知および強化のためのコンテキス
			ータ管理	トデータソースを管理する。
		8.3 サービス:コ	8.3.3 機能:実装	状況の変化に対してさらなる準備や
		ミュニケーショ		対応をするためにコミュニケーショ
		ン		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	「深堀分析ツール運用」サ	N/A		
ール運用	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。			
G-9. 分析基盤基	「分析基盤基本運用」サー	N/A		
本運用	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。			
G-10. 分析基盤	「分析基盤高度運用」サー	5.1 サービス:監	5.1.2 機能:検知ユースケー	検知ユースケースのポートフォリオ
高度運用	ビスは、市販の SIEM では	視と検知	ス管理	を、ライフサイクル全体を通して管理
	取得できないシステムログ			する。

	ウットノナ・プナ・ブ			
	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	検知および強化のためのコンテキス
			ータ管理	トデータソースを管理する。
G-11. CDC シス	「CDC システム運用」サー	N/A		
テム運用	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。			
G-12. 既設セキ	「既設セキュリティツール	N/A		
ュリティツール	検証」サービスは、既に存在			
検証	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			

	田。の主に可用性の知点で			
	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	「新規セキュリティツール	7.3 サービス:脆	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
ュリティツール	検証」サービスは、セキュリ	弱性分析		め、または脆弱性が悪用される影響を
検証	ティ活動において新たな対			緩和(軽減)するために必要な手順を開
	策が必要となった場合に、			発する。
	新規のセキュリティ資産の			
	設計・導入を実現する。			
H-1. 内部不正対	「内部不正対応・分析支援」	6.4 サービス:緩	6.4.4 機能:他の情報セキュ	情報セキュリティインシデントを適
応・分析支援	サービスは、内部不正が発	和と回復	リティエンティティの支援	切に緩和し、また情報セキュリティイ
	覚した場合に、セキュリテ			ンシデントから回復するために必要
	ィ活動で取得したログから			な管理および技術的活動を、コンステ
	行動内容を整理すること			ィチュエンシーが実行できるように
	で、組織的な対応を支援す			する。
	る。			
H-2. 内部不正検	「内部不正検知・再発防止	N/A		
知·再発防止支援	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。			
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	発	集約	予防・緩和のために、コンスティチュ
		光	朱祁	
	係者の意識を高め、ビジネ			エンシーに伝えられる情報を集約、照
	ス資産を保護するための適			合して、優先順位を付ける。
	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	異なる対象者にリーチする、または特
			発資料の作成	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	「教育・トレーニング」サー	6.4 サービス:緩	6.4.4 機能:他の情報セキュ	情報セキュリティインシデントを適
ニング	ビスは、CDC が支援する組	和と回復	リティエンティティの支援	切に緩和し、また情報セキュリティイ
	織関係者への、セキュリテ			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			な管理および技術的活動を、コンステ
ングを支援する。			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	9.2.1 機能:知識、スキル、能	必要な KSA に関してコンスティチュ
	レーニングと教	力要件の収集	エンシーのニーズを適切に評価、特
	育		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	コンスティチュエンシーの KSA ニー
		ーニング資料の開発	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	CSIRT が、様々な対象者とコンテン
		信	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	スタッフメンバーが適切な計画を立
			の専門的能力開発	ててキャリア形成を成功させること
			の一世 1471年7月 元	ができるよう支援する。
10 by 115		0.4.11 187.44	011機化・壮生マルバノコ	
I-3. セキュリテ	「セキュリティコンサルテ	9.4 サービス:技	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
イコンサルティ	ィング」サービスは、ビジネ	術およびポリシ		活動を可能にする一方で、コンスティ
ング	スにおけるさまざまな業務	ーに関するアド		チュエンシーがリスクと脅威をより
	で、セキュリティに関連し	バイス		よく管理し、現在の運用とセキュリテ
	たコンサルティングを実現			ィのベストプラクティスを実装でき
	する。			るような技術的アドバイスを提供す
	9 3 .			వ .
I-4. セキュリテ	「セキュリティベンダー連	N/A		
ィベンダー連携	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			
T = 1 1 2 =	5. In 12 - 12 - 12 - 12 - 12 - 12 - 12 - 12	- 1 1 20 - 14		V all a OTT d) a set to v
I-5. セキュリテ	「セキュリティ関連団体と	7.4 サービス:脆	7.4.1 機能:脆弱性の通知・報	その他の CVD プロセスの関係者に
ィ関連団体との	の連携」サービスは、外部の	弱性の調整	告	新しい脆弱性情報を最初に共有また

N-Le LVI.				. S. Den et . S. Lea
連携	コミュニティへの参加を通			は報告する。
	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	協調的な脆弱性の公開(CVD)の取り
			者の調整	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	8.3.1 機能:組織内外とのコ	現在の状況とそれがどのように変化
		ミュニケーショ	ミュニケーション	しているかをコンスティチュエンシ
		ン		ー(およびその他)に知らせる。
			8.3.4 機能:普及・統合・情報	情報を集め、標準化し、準備し、コン
			共有	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	幹部向けセキュリティ報	N/A	
キュリティ報告	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。		

2. FIRST CSIRT Services Framework version 2.1.0 への対応

FIRST CSIRT Ser	vices Framework v	rersion 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	5.1.1 機能:ログ	ログソースとセンサーを管理す	G-1. セキュリティ	「セキュリティアーキテクチャ実装」サ
視と検知	とセンサーの管	る。	アーキテクチャ実装	ービスは、CDC の戦略マネジメント (カ
	理			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	「ネットワークセキュリティ製品基本運
			セキュリティ製品基	用」サービスは、ファイアウォール、不正
			本運用	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	「エンドポイントセキュリティ製品基本
			トセキュリティ製品	運用」サービスは、アンチウイルスソフト
			基本運	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	「クラウドセキュリティ製品基本運用」
			ュリティ製品基本運	サービスは、クラウドで提供されるセキ
			用	ュリティサービスの運用を実現する。
	5.1.2 機能:検知	検知ユースケースのポートフォ	F-1. 事後分析	「事後分析」サービスは、CDC 関係者の
	ユースケース管	リオを、ライフサイクル全体を		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
生			
			現する。
		G-3. ネットワーク	「ネットワークセキュリティ製品高度運
		セキュリティ製品高	用」サービスは、IDS/IPS や WAF など
		度運用	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	「エンドポイントセキュリティ製品高度
		トセキュリティ製品	運用」サービスは、エンドポイント内の不
		高度運用	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	「クラウドセキュリティ製品高度運用」
		ュリティ製品高度運	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	「分析基盤高度運用」サービスは、市販の
		運用	SIEM では取得できないシステムログや
		Æ/11	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	検知および強化のためのコンテ	G-3. ネットワーク	「ネットワークセキュリティ製品高度運
テキストデータ	キストデータソースを管理す	セキュリティ製品高	用」サービスは、IDS/IPS や WAF など
管理	る。	度運用	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	「エンドポイントセキュリティ製品高度
		トセキュリティ製品	運用」サービスは、エンドポイント内の不
		高度運用	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	「クラウドセキュリティ製品高度運用」
		ュリティ製品高度運	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	「分析基盤高度運用」サービスは、市販の
			運用	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	5.2.1 機能:関連	他の潜在的または進行中のセキ	B-1. リアルタイム	「リアルタイム監視」サービスは、ログや
ベント分析	付け	ュリティインシデントに直接関	監視	ネットワークフローからシステムの状態
		連するイベントを特定する。		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	真陽性の検知を特定、分類し、優	B-1. リアルタイム	「リアルタイム監視」サービスは、ログや
	性確認	先順位付けするために、検知さ	監視	ネットワークフローからシステムの状態
		れた潜在的な情報セキュリティ		や不審な動きを監視・分析し、インシデン
		インシデントをトリアージして		トやイベントに応じて必要な情報を収集
		適格性を確認する。		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	セキュリティイ	第三者から報告された、情報セ	報告受付	用における分析報告の受け付けを実現す
インシデント報	ンシデント報告	キュリティインシデントに関す	TK 11 2/13	る。報告の受領は組織内部からだけでは
	. , , , , ,	, , , , , , , , , , , , , , , , , , , ,		
告の受付	の受理	る情報を受付または受理する。		なく、外部の組織からの場合もある。
	6.1.2 機能:情報	報告された情報セキュリティイ	D-2. インシデント	 「インシデントハンドリング」サービス
	セキュリティイ	ンシデントについて、初めにレ	ハンドリング	_
	ンシデントのト	ビュー、分類、優先順位付け、お		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。
	リアージと処理	よび処理を行う。		3 かり D-1 の信勤の調金を天残する。
6.2 サービス:情	6.2.1 機能:情報	情報セキュリティインシデント	D-3. インシデント	 「インシデント分類 サービスは、発生し
報セキュリティ	セキュリティイ	を分類し、優先順位を付け、初期	分類	「インシアントカ頬」
インシデントの	ンシデントのト	評価を行う。		
分析	リアージ(優先順			て共通理解を促すために、インシデント
	位付けと分類)			の分類を実現する。
	6.2.2 機能:情報	情報セキュリティインシデント	D-3. インシデント	
	収集	およびその一部とみなされるす	分類	「インシデント分類」サービスは、発生し
		べての情報セキュリティイベン		たインシデントとその原因の種別につい
		トに関連する情報を取得し、カ		て共通理解を促すために、インシデント
		タログを作成し、保存および追		の分類を実現する。
		跡する。		
	6.2.3 機能:詳細	インシデントに関するその他の	D-3. インシデント	「インシデント分類」サービスは、発生し
	分析の調整	技術分析を開始して追跡する。	分類	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	するため、悪用された脆弱性が	対応・封じ込め	は、インシデントがすべてのリソースに
	ンシデントの根	存在したり、悪用が成功したり		 広がるなど、被害や影響が拡大する前の
	本原因分析	するのを許してしまった状況(ユ		封じ込めを実現する。
	1	ーザーの行動を含むが、それに		
		限定されない)を特定する。		
	6.2.5 機能:クロ	利用可能なすべての情報を使っ	F-1. 事後分析	
	スインシデント	て、コンテキストを最大限に理		「事後分析」サービスは、CDC 関係者の
	相関	解し、それ以外の方法では認識		手順やツールの見直しや改善を実現する
		されなかった、または対処でき		ため、インシデントの解決法の詳述を実
		なかった相互関係を検知できる		現する。
		ようにする。		
6.3 サービス:ア	6.3.1 機能: メデ	アーティファクトから収集され	C-1. フォレンジッ	「フォレンジック分析」サービスは、何が
ーティファクト	ィアまたはサー	た情報を、他のパブリックおよ	ク分析	発生したのかの判断を促進するため、セ
とフォレンジッ	フェス分析	びプライベートのアーティファ		キュリティ関連資産から収集された、あ
ク痕跡の分析		クトや署名リポジトリと比較す		るいはイベントに関連したデジタル証跡
		る。		の分析を実現する。
	6.3.2 機能:リバ	アーティファクトの完全な機能	C-2. 検体解析	「検体解析」サービスは、フォレンジック
	ース・エンジニア	を、その実行環境に関係なく断		の過程で発見された、攻撃者によって設
	リング	定するために、アーティファク		置されたマルウェア、プログラムやスク
		トの詳細な静的分析を行う。		リプトの解析を実現する。
	6.3.3 機能:ラン	アーティファクトの操作に関す	C-2. 検体解析	「検体解析」サービスは、フォレンジック
	タイムまたは動	る洞察を提供する。		の過程で発見された、攻撃者によって設
	的解析			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	カタログ化されたアーティファ	C-3. 追及・追跡	「追及・追跡」サービスは、環境に対する
	分析	クトのファミリー分析など、共		あらゆる攻撃の発生源を追及・追跡を実
		通の機能または意図の特定に重		現するもので、これはセキュリティイン
		点を置いた分析を行う。		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	6.4.1 機能:対応	影響を受けたシステムの完全性	D-4. インシデント	
和と回復	計画の策定	を回復し、影響を受けたデータ、	対応・封じ込め	
		システム、およびネットワーク		 「インシデント対応・封じ込め」 サービス
		を劣化していない動作状態に戻		は、インシデントがすべてのリソースに
		し、元のセキュリティ問題が再		広がるなど、被害や影響が拡大する前の
		び悪用されるコンテキストを再		封じ込めを実現する。
		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	情報セキュリティインシデント		 「インシデント対応・封じ込め」 サービス
	的な対策と封じ	がこれ以上拡大しない、すなわ	対応・封じ込め	は、インシデントがすべてのリソースに
	込め	ち、現在影響を受けているシス		広がるなど、被害や影響が拡大する前の
		テムやユーザー、ドメインに限		封じ込めを実現する。
		定して、これ以上の損失(文書の		11112121000

		\(\text{\tinc{\text{\tin}\exiting{\text{\tin}\tint{\text{\ti}\tinity}}\\ \text{\text{\text{\text{\text{\text{\text{\text{\tetx{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\tin\tint{\text{\text{\text{\text{\text{\ti}\tinit{\text{\ti}\tin{\text{\ti}\tint{\text{\tin}\tint{\text{\tin}\text{\text{\t		
		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	影響を受けたドメインやインフ	D-5. インシデント	「インシデント復旧」サービスは、対象と
	テムの復旧	ラストラクチャ、ネットワーク	復旧	なるシステムを通常状態へ回復すること
		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。		を支援する。
	6.4.4 機能:他の	情報セキュリティインシデント	D-5. インシデント	
	情報セキュリテ	を適切に緩和し、また情報セキ	復旧	
	イエンティティ	ュリティインシデントから回復		「インシデント復旧」サービスは、対象と
	の支援	するために必要な管理および技		なるシステムを通常状態へ回復すること
		術的活動を、コンスティチュエ		を支援する。
		ンシーが実行できるようにす		
		る。		
			H-1. 内部不正対応・	「内部不正対応・分析支援」サービスは、
			分析支援	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	6.5.1 機能:コミ	利害関係者と効果的に連携し、	D-6. インシデント	「インシデント通知」サービスは、インシ
報セキュリティ	ュニケーション	必要とされる機密性を提供す	通知	デント対応チームやその他関連するグル
インシデントの		る、適切な複数のコミュニケー		ープに対して、インシデント発生の伝達
調整		ションチャネルを確立する。		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	D-6. インシデント 通知	
	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		「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	もらうのに必要な情報を提供する。 特定されたエンティティとのコ	D-6 インシデント	
情報の配信	マ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。		「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	

		サウル フのは Eママ4 と 日立	1-1-1-4-11 H-	± 12± → 1
		決定が、その時点で可能な最良	対応報告	応が完了したインシデントのレポートの
		の状況把握に基づくよう、事業		完成と報告を実現する(対策の試みが長
		内のすべての関係エンティティ		期化する場合は、CDC の戦略マネジメン
		が、確実に現在の活動状況に関		ト (カテゴリーA) に引き継がれる)。イ
		する情報を持っているようにす		ンシデント対応中に CDC 関係者が現状
		る。		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	風評や誤解を招くような情報の	D-7. インシデント	「インシデント対応報告」サービスは、対
	イアとのコミュ	流布を避けるために、進行中の	対応報告	応が完了したインシデントのレポートの
	ニケーション	イベントに関する正確で分かり		完成と報告を実現する(対策の試みが長
		やすい、事実に基づいた情報を		期化する場合は、CDC の戦略マネジメン
		提供できるように(公共の)メデ		ト (カテゴリーA) に引き継がれる)。イ
		ィアと連携する。		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	6.6.1 機能:コン	危機への対処を支援するために	D-6. インシデント	「インシデント通知」サービスは、インシ
機管理支援	スティチュエン	確立されたコミュニケーション	通知	デント対応チームやその他関連するグル
	シーへの情報配	リソースを提供する。		ープに対して、インシデント発生の伝達
	信			を実現する。
	6.6.2 機能:情報	危機管理チームが、現在の情報	D-6. インシデント	「インシデント通知」サービスは、インシ
	セキュリティの	セキュリティインシデントと既	通知	デント対応チームやその他関連するグル
	状況報告	知の脆弱性の完全な概要を把握		ープに対して、インシデント発生の伝達
		し、これを全体的な優先事項と		を実現する。

		温吹の 切しして投票でもフト		
		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	現在起きている情報セキュリテ	D-6. インシデント	 「インシデント通知 サービスは、インシ
	的意思決定の伝	ィインシデントに対して危機が	通知	_ · · · · · · · · · · · · · · · · · · ·
	達	与える影響について、他のエン		デント対応チームやその他関連するグル
		ティティにタイムリーに情報提		一プに対して、インシデント発生の伝達
				を実現する。
		供する。		
7.1 サービス:脆	7.1.1 機能:イン	セキュリティインシデントの一	D-6. インシデント	「インシデント通知」サービスは、インシ
弱性の発見・調査	シデント対応の	部として悪用された脆弱性を特	通知	デント対応チームやその他関連するグル
	脆弱性発見	定する。		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	「内部脅威情報の収集・分析」サービス
			の収集・分析	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	公的情報源またはその他の第三	F-3. 外部脅威情報	「外部脅威情報の収集・評価」サービス
	情報源による脆	者の情報源を参照して、新しい	の収集・評価	は、新たな脆弱性、攻撃の傾向、マルウェ
	弱性の発見	脆弱性について知る		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	意図的な活動または調査の結果	E-3. 脆弱性診断	「脆弱性診断」サービスは、ネットワー
	性調査	として、新しい脆弱性を発見ま		ク、システム、アプリケーションの脆弱性
		たは探索する。		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	「ペネトレーションテスト」サービスは、
			ョンテスト	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	高度サイバー攻撃(APT)に対抗するため
			攻擊耐性評価	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)。
7.2 サービス:脆	7.2.1 機能:脆弱	コンスティチュエンシーまたは	F-2. 内部脅威情報	「内部脅威情報の収集・分析」サービス
弱性報告の取得	性報告の受理	第三者から報告された脆弱性に	の収集・分析	は、リアルタイム分析やインシデント対
		関する情報を受付または受理す		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	「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。
	7.2.2 機能:脆弱	脆弱性報告の初期レビュー、分	F-2. 内部脅威情報	「内部脅威情報の収集・分析」サービス
	性報告のトリア	類、優先順位付け、および処理を	の収集・分析	は、リアルタイム分析やインシデント対
	ージと処理	行う。		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。
7.3 サービス:脆	7.3.1 機能:脆弱	脆弱性を分類し、優先順位を付	F-2. 内部脅威情報	「内部脅威情報の収集・分析」サービス
弱性分析	性のトリアージ	け、初期評価を行う。	の収集・分析	は、リアルタイム分析やインシデント対
	(検証と分類)			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。
7.3.2 機能:脆弱	脆弱性の原因となった、または	F-2. 内部脅威情報	「内部脅威情報の収集・分析」サービス
性の根本原因分	その存在を顕在化する設計上ま	の収集・分析	は、リアルタイム分析やインシデント対
析	たは実装上の欠陥を理解する。		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。
7.3.3 機能:脆弱	潜在的な脆弱性を修正(是正)す	F-2. 内部脅威情報	「内部脅威情報の収集・分析」サービス
性対策開発	るため、または脆弱性が悪用さ	の収集・分析	は、リアルタイム分析やインシデント対
	れる影響を緩和(軽減)するため		応に関する情報 (内部インテリジェンス)
	に必要な手順を開発する。		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。
		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

			1	
			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	7.4.1 機能:脆弱	その他の CVD プロセスの関係	I-5. セキュリティ関	「セキュリティ関連団体との連携」サー
弱性の調整	性の通知・報告	者に新しい脆弱性情報を最初に	連団体との連携	ビスは、外部のコミュニティへの参加を
		共有または報告する。		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	協調的な脆弱性の公開(CVD)の	I-5. セキュリティ関	「セキュリティ関連団体との連携」サー
	性利害関係者の	取り組みに関与する様々な利害	連団体との連携	ビスは、外部のコミュニティへの参加を
	調整	関係者および参加者の間で継続		通じて、積極的な情報交換を実現する。そ
		した調整と情報共有を行う。		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	7.5.1 機能:脆弱	CSIRT が脆弱性をハンドリン	A-3. ポリシーの企	
弱性の開示	性開示ポリシー	グして開示する方法、および脆	画立案	「ポリシーの企画立案」 サービスは、 具体
	とインフラスト	弱性を開示するために使用され		7 7 7 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	ラクチャの整備	るメカニズムについて、フレー		的なセキュリティポリシーの定義や、ガ
		ムワークを提供し、期待値を設		イドラインの作成に関するすべての活動
		定するポリシーを策定し、維持		を支援する。
		する。		
	7.5.2 機能:脆弱	脆弱性を検知、修正、または緩和	F-5. 脅威情報の活	「脅威情報の活用」サービスは、あらゆる
	性の公表・連絡・	し、将来の脆弱性の不正利用を	用	カテゴリーのセキュリティ対応のため
	周知	防止できるようにコンスティチ		に、脅威情報の編纂と発信を実現する。

	7.5.3 機能:脆弱 性開示後のフィ ードバック	ュエンシー(または一般の人々) に情報を提供する。 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。	, , , , , , , , , , , , , , , , , , , ,	「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、	既存の資産、コンスティチュエ	E-2. 資産棚卸	
	役割、アクショ	ンシー、ベースラインおよび期	五 2. 英座顺即	「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
		待される活動の知識を提供する		るシステム、アセット、アプリケーション
	の資産のマッピ	ことで、異常な状況の観察を特		 の全数調査の情報管理を実現する。
	ング	定する分析機能を支援する。		
	8.1.3 機能:収集	分析・解釈サービスや他の	F-2. 内部脅威情報	「内部脅威情報の収集・分析」サービス
		CSIRT サービスを支援するた	の収集・分析	は、リアルタイム分析やインシデント対
		めに情報を収集する。		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。
	8.1.4 機能:デー	CSIRT 活動および分析サービ	F-5. 脅威情報の活	「森子陸却の江田」は、18つは、まとはフ
	タ処理と準備	スの要件をサポートできる、信	用	「脅威情報の活用」サービスは、あらゆる
		頼性と一貫性のある最新のデー		カテゴリーのセキュリティ対応のため
		タセットを確立する。		に、脅威情報の編纂と発信を実現する。
8.2 サービス:分	8.2.1 機能:予測	現在の状況の特定または将来の	F-2. 内部脅威情報	「内部脅威情報の収集・分析」サービス
析と統合	と推定	状況の予測を目的として、デー	の収集・分析	は、リアルタイム分析やインシデント対
		タ取得中に収集された情報を分		応に関する情報(内部インテリジェンス)
		析する。		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	コンスティチュエンシーの現在	B-1. リアルタイム	「リアルタイム監視」サービスは、ログや
	ント検知(アラー	の状況の詳細を断定し、確認す	監視	ネットワークフローからシステムの状態
	トや探索を通じ	る。		や不審な動きを監視・分析し、インシデン
	て)			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	被害を抑制し、将来のリスクを	D-2. インシデント	
	セキュリティイ	緩和する、あるいは新しく発生	ハンドリング	「インシデントハンドリング」サービス
	ンシデントマネ	した弱点を特定するのに役立つ		は、受け付けたインシデントに対処し、D-
	ジメントの意思	かもしれない新しい見識をイン		3 から D-7 の活動の調整を実現する。
	決定支援	シデント中に特定する。		
	8.2.4 機能:状況	現在観察されている事象や今後	D-2. インシデント	「インシデントハンドリング」サービス
	的影響	観察されうる事象が状況図に与	ハンドリング	「インシノンドハンドリンク」リーにA は、受け付けたインシデントに対処し、D-
		えると予想される潜在的影響を		は、受り付りたインシケントに対処し、 D -13から D-7 の活動の調整を実現する。
		決定する。		3 149 17 17 17 17 17 17 19 19 19 19 19 19 19 19 19 19 19 19 19
8.3 サービス:コ	8.3.1 機能:組織	現在の状況とそれがどのように	I-5. セキュリティ関	「セキュリティ関連団体との連携」サー
ミュニケーショ	内外とのコミュ	変化しているかをコンスティチ	連団体との連携	ビスは、外部のコミュニティへの参加を
ン	ニケーション	ュエンシー(およびその他)に知		通じて、積極的な情報交換を実現する。そ
		らせる。		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	結果、アーティファクトまたは	F-4. 脅威情報報告	
と推奨事項	所見を作成し、分析中に発見ま		「脅威情報報告」サービスは、内部と外部
	たは作成された重大な情報を、		の脅威情報を取りまとめ、詳細も含めた
	受取手が理解できる方法と形式		ドキュメント化を実現する。
	で伝える。		
8.3.3 機能:実装	状況の変化に対してさらなる準	G-1. セキュリティ	「セキュリティアーキテクチャ実装」サ
	備や対応をするためにコミュニ	アーキテクチャ実装	ービマュリティテーキテクリヤ美級」リービスは、CDC の戦略マネジメント (カ
	ケーションに基づいてコンステ		テゴリーA) で設計したセキュリティアー
	ィチュエンシーの環境を調整す		ナコリーA) (設計したビャュリティアート) キテクチャの実装を実現する。
	る。		イプラブヤの大赦を失先する。
		G-3. ネットワーク	「ネットワークセキュリティ製品高度運
		セキュリティ製品高	用」サービスは、IDS/IPS や WAF など
		度運用	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	「エンドポイントセキュリティ製品高度
		トセキュリティ製品	運用」サービスは、エンドポイント内の不
		高度運用	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	「クラウドセキュリティ製品高度運用」
		ュリティ製品高度運	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。
8.3.4 機能:普及·	情報を集め、標準化し、準備し、	I-5. セキュリティ関	「セキュリティ関連団体との連携」サー
統合•情報共有	コンスティチュエンシーおよび	連団体との連携	ビスは、外部のコミュニティへの参加を
	それ以外の人々と共有する。		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	情報の移転が成功し、使用可能	I-5. セキュリティ関	「セキュリティ関連団体との連携」サー
共有の管理	であることを確実にする。	連団体との連携	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	内部および外部の情報源から受	I-5. セキュリティ関	「セキュリティ関連団体との連携」サー
ードバック	信されるデータの品質、タイム	連団体との連携	ビスは、外部のコミュニティへの参加を
	リーさ、正確性および関連性を		通じて、積極的な情報交換を実現する。そ
	改善する。		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	9.1.1 機能:調査	セキュリティ態勢の改善とリス	I-1. 意識啓発	「意識啓発」サービスは、CDC に関わる
発	および情報集約	クの予防・緩和のために、コンス		あらゆる関係者の意識を高め、ビジネス
		ティチュエンシーに伝えられる		資産を保護するための適切なツール、ベ
		情報を集約、照合して、優先順位		ストプラクティス、ポリシー、リソースの
		を付ける。		活用促進を実現する。
	9.1.2 機能:報告	異なる対象者にリーチする、ま	I-1. 意識啓発	
	書および啓発資	たは特定のコンテンツを可能な		「意識啓発」サービスは、CDC に関わる
	料の作成	限り最善の方法で配信すること		あらゆる関係者の意識を高め、ビジネス
		を目標とし、関連性があるもの		資産を保護するための適切なツール、ベ
		として収集・調査した情報を使		ストプラクティス、ポリシー、リソースの
		用して、異なるメディアで資料		活用促進を実現する。
		を作成する。		
	9.1.3 機能:情報	セキュリティプラクティスにつ	I-1. 意識啓発	「意識啓発」サービスは、CDC に関わる
	の普及	いての認識とプラクティスの実		あらゆる関係者の意識を高め、ビジネス
		装を改善するために、セキュリ		資産を保護するための適切なツール、ベ
		ティに関連する情報を普及させ		ストプラクティス、ポリシー、リソースの
		る。		活用促進を実現する。
	9.1.4 機能:アウ	CSIRT のミッションの遂行を	I-1. 意識啓発	「意識啓発」サービスは、CDC に関わる
	トリーチ	支援する、またはミッションに		あらゆる関係者の意識を高め、ビジネス
		関わる可能性のある専門家また		資産を保護するための適切なツール、ベ
		は組織との関係を構築および維		ストプラクティス、ポリシー、リソースの
		持する。		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	スキル、能力要件	ィチュエンシーのニーズを適切	ング	が支援する組織関係者への、セキュリテ
育	の収集	に評価、特定、文書化し、適切な	•	ィ分野に特化したトレーニングを支援す
Ħ	· 分权来	トレーニングおよび教育資料を		
				る。
		開発してスキルレベルを改善す		
		る。		
	9.2.2 機能:教育	コンスティチュエンシーの KSA	I-2. 教育・トレーニ	
	およびトレーニ	ニーズを基に、様々な対象にリ	ング	「教育・トレーニング」サービスは、CDC
	ング資料の開発	ーチする、または特定のコンテ		が支援する組織関係者への、セキュリテ
		ンツを配信する上で最善とされ		ィ分野に特化したトレーニングを支援す
		る配信方法に適した教育、指導、		る。
		トレーニング資料を開発する。		
	9.2.3 機能:コン	CSIRT が、様々な対象者とコン	I-2. 教育・トレーニ	
	テンツの配信	テンツの特性に基づいて、コン	ング	「教育・トレーニング」サービスは、CDC
		スティチュエンシーにコンテン		が支援する組織関係者への、セキュリテ
		ツを最適に配信できるようにな		ィ分野に特化したトレーニングを支援す
		るコンテンツ配信のための正式		る。
		なプロセスを開発する。		
	9.2.4 機能:メン	CSIRT スタッフ、コンスティチ	I-2. 教育・トレーニ	
	タリング	ュエンシーまたは外部の信頼で	ング	「教育・トレーニング」サービスは、CDC
		きるパートナーが、確立された		が支援する組織関係者への、セキュリテ
		関係を通じて経験豊富なスタッ		ィ分野に特化したトレーニングを支援す
		フから学ぶためのプログラムを		る。
		開発する。		

	9.2.5 機	スタッフメンバーが適切な計画	I-2. 教育・トレーニ	「教育・トレーニング」サービスは、CDC
	能:CSIRT スタ	を立ててキャリア形成を成功さ	ング	が支援する組織関係者への、セキュリテ
	ッフの専門的能	せることができるよう支援す		ィ分野に特化したトレーニングを支援す
	力開発	る。		る。
9.3 サービス:演	9.3.1 機能:要件	演習の、あらかじめ決められた	E-6. 高度サイバー	高度サイバー攻撃(APT)に対抗するため
羽首	分析	範囲と焦点の特定の課題に集中	攻擊耐性評価	の「高度サイバー攻撃耐性評価」サービス
		することにより、確実に十分な		は、標的型メール訓練やソーシャルエン
		成果を得られるようにする。		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)。
	9.3.2 機能:フォ	演習の実施に必要な内部および	E-6. 高度サイバー	高度サイバー攻撃(APT)に対抗するため
	ーマットと環境	外部のリソースとインフラスト	攻擊耐性評価	の「高度サイバー攻撃耐性評価」サービス
	の開発	ラクチャを特定および決定す		は、標的型メール訓練やソーシャルエン
		る。		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、

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 E-6. 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」サービスと機能の効率と有効性、およ	1	T			at the control of the
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、 (サーバー攻撃対応演習と呼ぶ)。 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-7. サイバー攻撃 「サイバー攻撃対応力評価」サービスは、標的型メール訓練やソーシャルエージニアリングテストを実施しながら、対象を対象者に提供する。 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、
9.3.3 機能:シナ 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(APT)に対抗するための「高度サイバー攻撃耐性評価」サービ、は、標的型メール訓練やソーシャルエージニアリングテストを実施しながら、おめ型攻撃に対する組織耐性の計測を実施しながら、おりであると対象者に提供する。 E-7. サイバー攻撃 「サイバー攻撃対応力評価」サービスは、	1	1			セキュリティ対応が実際に発動され、イ
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(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ージニアリングテストを実施しながら、物型攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施しながら、物理攻撃に対する組織耐性の計測を実施した。	1				ンシデントを遅滞なく終息させることが
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(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ージニアリングテストを実施しながら、もり型攻撃に対する組織耐性の計測を実施しながら、もり型攻撃に対する組織耐性の計測を実施しながら、もりである。	1				できるかどうかの確認を実現する(サイ
サオ開発 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。 「高度サイバー攻撃が性評価」サービ は、標的型メール訓練やソーシャルエー ジニアリングテストを実施しながら、 的型攻撃に対する組織耐性の計測を実 する。 「サイバー攻撃対応力評価」サービスは	1				バー攻撃対応演習と呼ぶ)。
サオ開発 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-7. サイバー攻撃 「サイバー攻撃対応力評価」サービスは で 「高度サイバー攻撃耐性評価」サービ は、標的型メール訓練やソーシャルエジニアリングテストを実施しながら、 がも、 がとのスキル、知識、能力を改善する。 「サイバー攻撃対応力評価」サービスは で 「サイバー攻撃対応力評価」 サービスは 「サイバー攻撃対応力評価」 サービスは 「サイバー攻撃対応力評価」 サービスは 「サイバー攻撃対応力評価」 サービスは 「サイバー攻撃対応力評価」 サービスは 「カイバー攻撃対応力評価」 サービスは 「サイバー攻撃対応力評価」 「サイバー攻撃対応力評価」 「サイバー攻撃対応力評価」 「サイバー攻撃対応力評価」 「サイバー攻撃対応力評価」 「サイバー攻撃対応力評価」 「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 「サイバー攻撃対応力評価」 「サービスは 「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 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		9.3.3 機能:シナ	コミュニケーションの観点を含	E-6. 高度サイバー	古中山ノジ 内部(ADM))z 牡ゼナフをル
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-7. サイバー攻撃 「サイバー攻撃対応力評価」サービスは	1	リオ開発	む、模擬サイバーセキュリティ	攻擊耐性評価	
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。	1		イベントやインシデントのハン		
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。	1		 ドリングを通して、そのサービ		
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-7. サイバー攻撃 「サイバー攻撃対応力評価」サービスは	1	1	 スと機能の効率と有効性、およ		ジニアリングテストを実施しながら、標
する機会を対象者に提供する。	1				的型攻撃に対する組織耐性の計測を実現
E-7. サイバー攻撃 「サイバー攻撃対応力評価」サービスは	1	1			する。
		-	うる成式で対象名に歴伝する。	ロロ ルノバ 安報	「ルノッ・投載場合工事」ルーパッル
対応力評価	1				
	1			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、	1				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	1				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	1				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)。					バー攻撃対応演習と呼ぶ)。
9.3.4 機能:演習 CSIRT チームが組織の CSIRT E-6. 高度サイバー 高度サイバー攻撃(APT)に対抗するた		9.3.4 機能:演習	CSIRT チームが組織の CSIRT	E-6. 高度サイバー	高度サイバー攻撃(APT)に対抗するため
の実行 計画の妥当性とその実行能力に 攻撃耐性評価 の「高度サイバー攻撃耐性評価」サービ		の実行	計画の妥当性とその実行能力に	攻擊耐性評価	の「高度サイバー攻撃耐性評価」サービス
対する信頼を高めるためにドリ は、標的型メール訓練やソーシャルエ			対する信頼を高めるためにドリ		は、標的型メール訓練やソーシャルエン
ル・演習を実施する。 ジニアリングテストを実施しながら、			ル・演習を実施する。		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		1	I .	I	

				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)。
	9.3.5 機能:演習	実際の観察に基づいて、演習の	E-6. 高度サイバー	高度サイバー攻撃(APT)に対抗するため
	成果レビュー	形式的で客観的な分析を行う。	攻擊耐性評価	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)。
9.4 サービス:技	9.4.1 機能:リス	情報セキュリティおよびその他	A-2. リスクアセス	「リスクアセスメント」サービスは、組織
術およびポリシ	クマネジメント	の関連機能と連携して、機会と	メント	の資産や脅威、セキュリティ対策の観点
ーに関するアド	支援	脅威の特定能力を改善し、統制・		から、組織のリスクレベル把握を実現す
バイス		管理を改善し、損失防止および		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	事業継続と災害復旧に関する信	A-5. 事業継続性	
継続および災害	頼されるアドバイザーとして、		「古光処体界」よ、びった。如体の古光処
復旧計画の支援	中立的で事実に基づいたアドバ		「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
	イスを提供し、そのアドバイス		統計画の美境や美行が正しく行われるに めに必要な経営上の機能を支援する。
	を使用できる環境と適用される		のに必要は経営工の機能を又援する。
	リソースの制約を考慮する。		
9.4.3 機能:ポリ	アドバイスが利用される可能性	A-3. ポリシーの企	
シーの支援	のある環境および適用されるリ	画立案	
	ソースの制約を考慮し、公平で		「ポリシーの企画立案」サービスは、具体
	事実に基づいたアドバイスを提		的なセキュリティポリシーの定義や、ガ
	供することにより、ポリシーの		イドラインの作成に関するすべての活動
	開発および実施について信頼さ		を支援する。
	れるアドバイザーとして行動す		
	る。		
9.4.4 機能:技術	効果的なインシデントハンドリ	I-3. セキュリティコ	
アドバイス	ング活動を可能にする一方で、	ンサルティング	 「セキュリティコンサルティング」サー
	コンスティチュエンシーがリス		「セキュリティコンサルティンク」リ ビスは、ビジネスにおけるさまざまな
	クと脅威をよりよく管理し、現		それ、こう不ろにおりるごまごまな来
	在の運用とセキュリティのベス		傍じ、ピキュリティに関連したコンリル ティングを実現する。
	トプラクティスを実装できるよ		ノインフセ天処りる。
	うな技術的アドバイスを提供す		

	る。		
N/A		A-1. リスクマネジ	「リスクマネジメント」サービスは、リス
		メント	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	「事業影響度分析」のサービスは、様々な
		析	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	「セキュリティアーキテクチャ設計」サ
		アーキテクチャ設計	ービスは、ビジネスをセキュアにするた

			T
			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	「トリアージ基準管理」サービスは、全社
		準管理	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

	T	
	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	「イベントデータ保管」サービスは、セキ
	タ保管	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	「レポート問い合わせ対応」サービスは、
	合わせ対応	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	「ネットワーク情報収集」サービスは、保
	情報収集	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	「深堀分析ツール運用」サービスは、デジ
	ル運用	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	「分析基盤基本運用」サービスは、必要な
	運用	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。

NT/A		C 11 CDC 3/7 =	「CDC ショニン田田」 ルードコル トル
N/A		G-11. CDC システ	「CDC システム運用」サービスは、これ
		ム運用	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	「既設セキュリティツール検証」サービ
		ティツール検証	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・	「内部不正検知・再発防止支援」サービス
		再発防止支援	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	「セキュリティベンダー連携」サービス
		ンダー連携	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	幹部向けセキュリティ報告」サービスは、
		リティ報告	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)