モンゴル国サイバーセキュリティ人材育成・研究開発環境整備計画にかかる情報収集・確認調査

ファイナルレポート

2024 年 12 月

独立行政法人

国際協力機構(JICA)

一般社団法人

JPCERT コーディネーションセンター

ガ平
JR
24-043

目次

第１章：調査の背景・経緯

過去 30 年間で飛躍的に普及した携帯電話とインターネットは世界的な情報化とデジタル経済の発展をもたらしている。一方、ヒト、モノ、カネ、組織やインフラシステムの多くがサイバー空間で繋がることにより、サイバーセキュリティのリスクも甚大化している。モンゴル国においても、デジタル化の推進とサイバーセキュリティの確保は表裏一体の重要な課題である。2020 年 5 月に国家大会議で承認された長期開発計画「ビジョン 2050」では、サイバーセキュリティに保護された革新的 ICT を開発し、国家能力の強化を目指している。また、モンゴル「新再生戦略」（2022 年 1 月）では、科学技術に基づいたハイテック、ブロックチェーン、人工知能の成果導入、デジタル経済の動向にあった産業化促進の記載があるが、サイバーセキュリティ分野のレジリエンス強化はデジタル経済の促進と密接な関係にある。 モンゴルは、2020 年 10 月に電子政府プラットフォームの E-Mongolia の稼働を開始した。更に、2022 年 4 月には情報技術庁がデジタル開発通信省（Ministry of Digital Development and Communications。以下「MDDC」という。）に昇格し、同年 5 月に「サイバーセキュリティ法」、「個人情報保護法」、「電子署名法」、「公共情報トランスペアレンシー法」が施行され、「国家デジタル戦略」が制定された。このようにモンゴルは国家デジタル社会の構築に向けて政策制度を急速に整備しようとしている。また、モンゴルでは産業の多様化が求められており、陸上輸送を必要としない ICT やデジタル産業の振興が期待されている。

このような状況の中、JICA はモンゴルにおけるサイバーセキュリティ教育プログラムの充実を図るため、MDDC と共同で「サイバーセキュリティ人材育成プロジェクト」（以下、本プロジェクト）を 2023 年に開始した。また、MDDC は、モンゴルの重要インフラの一部のサイバーセキュリティ対策を担当する Public CSIRT 設立に取り組んでおり、検討チームを設置している。JICA は、Public CSIRT のための支援、機材・設備の可能性について MDDC と協議している。MDDC の要請を検討するため、Public CSIRT 設立関係者及びモンゴルのサイバーセキュリティ関係者からの情報収集、Public CSIRT に必要な機材・設備の検討促進、我が国が協力可能な事項を検討すべく、必要な情報を収集・分析する。

モンゴル Public CSIRT が、モンゴル国民から信頼されるナショナル CSIRT 及びコーディネーションセンターを目指すために提供するサービスとして、以下改善策に記載の通り提案する。また、当該具備すべきサービスを踏まえ、Public CSIRT にて整備が望ましいと考えられる機材及びサービスを別添資料のとおり提

案する。なお、別添資料は JPCECRT/CC が現段階の情報を踏まえて提案する案であり、先方政府関係者、及び JICA と合意したものではない。

第 2 章：現状（2024 年 5 月時点）

デジタル開発通信省傘下の Public CSIRT は 2024 年 1 月 1 日に正式に稼働を開始した。2024 年 5 月時点でメンバー数は訪問時点で 22 名、法的には 52 名が拡張可能となっている。組織内には Administration チーム、Incident Response（IR）チーム、Cyber Attach Prevention チーム、Research and Analysis チームの４チームを設置することが法的に定められているが、2024 年 5 月の職員に対する聞き取り調査の時点では、各チームの業務内容や役割分担がまだ明確ではなかった（例えば、SOC を設置したいという希望はあるものの、Incident Response チームと Cyber Attach Prevention チームのどちらに設置するのかの、職員間での意思統一を図れていなかった）。オフィスは２つ存在し、片方のオフィスで IR チーム（及びコンサルタントの MNCERT/CC 職員）が、もう片方のオフィスでその他３チームが勤務している状態で、どちらのオフィスもまだ工事中であった。Public CSIRT としてサーバーは所有しておらず、またデータセンターにも存在しない。

これが一番の重要な点であるが、5 月の訪問時点で、IR チームに技術的な知識のあるメンバーがいなかった。現状、IR におけるほぼ全ての業務（情報収集・分析等）はコンサルタント契約をしている MNCERT/CC の職員が行っており、最終的な通知の部分のみ IR チームが行っている。また、MNCERT/CC 職員による Public CERT 職員の教育はコンサルタント契約上では ”optional” なものであり、義務ではないとのことであった。また、IR チームと MNCERT/CC は同じオフィスでも別々の部屋が割り当てられており、両者間のコミュニケーション手段は対面を除けばメールのみであった。

したがって、Public CISRT は、CSIRT 業務の根幹であるインシデントレスポンスについて技術的な知識を持つスタッフが存在しない点から、まだ CSIRT として機能しているとは言えず、国際的なサイバーセキュリティのコミュニティには参加できる段階ではないと考えられる。

また、モンゴルには Public CSIRT 以外にも General Intelligence Agency（GIA）傘下の National CSIRT、前述の MNCERT/CC、MonCIRT の３つの国家 CERT が存在した。National CSIRT は 2023 年に稼働開始した新生の国家 CERT で、メンバーは 2024 年 5 月の訪問時点で 12 名であった。職員数に法的な上限は無く、現在の予

算では 20 名まで拡張可能とのことであった。同組織には既にインシデント報告窓口が存在し、24 時間稼働する SOC も設置されていた。海外のトレーニング、CTF 等に参加経験があり、既に国際的な CSIRT コミュニティである FIRST にも加盟している。また、Google と共同で 8 週間の CS 教育プログラムを実施し、これまで 50 名が参加したとの話であった。以上を踏まえ、National CSIRT は既に CSIRT として十分に機能しており、国際的なサイバーセキュリティのコミュニティにも参加できるレベルに達していると言える。

MNCERT/CC は 2014 年から稼働している国家 CERT で、金融、通信、鉱業等から約 50 組織のメンバーから成るメンバーシップ組織である。コンスティチュエンシーはモンゴル国民全体であるものの、主にこのメンバーに対してサービス提供を行う。理事が 10 名、フルタイム職員が 7 名（内、5 名は Public CSIRT に常駐）在籍している。現状、Public CSIRT の IR 業務を実質的に行っているのはこの MNCERT/CC 職員であり、10 チケット/月程度のインシデント対応実績がある。

MonCIRT は、かつてはモンゴルの国家 CERT の一つであったが、2024 年 5 月の訪問で、既に CSIRT 業務を行っていないことが分かった。（代表の Khaltar 氏曰く、CSIRT 業務は MDDC へ移管したとのことであった。）現在は職員 3 名とともにサイバーセキュリティに関するコンサルタントサービスを提供する企業となっている。

以上の通り、モンゴルには Public CISRT の他にも、以前から存在していた MNCERT/CC、既に国家 CERT としての役目を終えた MonCIRT、Public CISRT よりも少し早く稼働を開始した National CSIRT が存在し、現状では Public CISRT の立ち遅れが目立つ。「CSIRT としてオペレーショナルな状態である」と言える状態にすることが急務であり、そのために以下の通り改善策を提案する。

第 3 章：改善策

まず、CSIRT の根幹ともいえるインシデント分析の一環として、インシデントの受付業務と OSINT (Open Source Intelligence)業務を行う。

前者では、113 ホットラインの拡充とフォーマライズを進める。専用の電話番号 113 を利用した相談窓口の設置についてはヒヤリング以前から Public CSIRT で進んでおり、一般に広く広報されてはいないものの、既に試験運用を開始しデ

ータの集積が始まっていた。JPCERT/CC にはこうした電話番号は無く、同様の業務を行っていないが、韓国インターネット振興院（KISA）には存在するため、特異な試みではない。この 113 ホットライン及び背後のデータベース拡充、インシデント受付業務をマニュアル化し、継続的・安定的に運用できるよう整備する。その際、Public CSIRT に期待されるのは、このホットラインに寄せられる個々の案件への対応ではなく、そこから見えるモンゴル全体のトレンドを掴むことであることに注意したい。

後者は公開情報を収集・分析してインテリジェンス業務として活用することを指す。セキュリティニュースサイト、セキュリティベンダの公開レポート、セキュリティアナリストの分析、公開されている IoC 情報、各国政府等の発表、サイバー攻撃を受けた組織からのプレスリリース、SNS 上の投稿等、大量の公開情報（合法的に入手可能なあらゆる情報）を毎日定常的に収集し、それらを突き合わせて分析することで、モンゴル国内及び海外でのセキュリティ関連のトレンドを、そのタイムラインとともに把握するように努める。また、ShadowServer からのレポートをレビューし、脆弱性のあるモンゴルのノードに通知する作業を行う。技術的要求が低く、特殊な機材を必要とせず、また時間とともに集積されていく情報にも価値があるため、Public CSIRT 職員には今日からでも開始してほしい業務である。（この一見ネットサーフィンにも思える作業が重要な業務であることは、2024 年 5 月の Public CSIRT 訪問時に既に Gantuya 氏、Amar 氏には直接伝えている。）

次に、モニタリングネットワーク”Eyes”の運用を行う。これは Zolbayar 代表及び Public CSIRT 職員から希望のあった「センサーを設置してモニタリングを行う」という業務にあたるものの、実現可能な形での提案である。具体的にはオープンソースのハニーポットツール “T-POT”を利用し、Public CSIRT 自身や MDDC のネットワークにセンサー（ハニーポット）を展開する。大学等の協力を得られる可能性もある。最初は最大 20 個程度のセンサーから始め、そうして設置したセンサーからの情報を Elastic Search や Kibana 等のツールを利用しダッシュボードやアタックマップとして表示しつつ、Public CSIRT 内部で徐々に分析の経験を積み重ねる。Zolbayar 代表が「我々はモンゴル国内で発生しているサイバー攻撃の情報を海外から得ており、自分たちの”目”が無い」と話していたことを受け、”Eyes”とした。ヒヤリング段階では「モンゴル国内の全 ISP に物理的なセンサーを設置」し、「全ての情報」を収集するという話であったが、具体的に何をどのように収集するのかがまだ不明瞭であった。また、モンゴル国内大手 ISP の中にはセンサー設置に抵抗感のある組織も存在した。サイバーセキュリティに

おいて、インシデント報告もその他の情報共有も、関係者からの信頼を得て初めて実現するものであり、Public CSIRT は今後モンゴル国民及び国内組織との信頼を、年月をかけて徐々に築き上げる必要がある。そのため、このスタートの段階から ISP と衝突するような事態や、何かを「強制してくる組織」だと思われるのは避けたいところである。

次に、IR チームはアーティファクト分析を行う。これには動的分析用、静的解析用、マルウェア保管用の基盤をそれぞれ用意し、これら分析環境はその他一般のオフィス環境とは別のネットワークとなっており、マルウェアをダウンロードするためのインターネット回線も別のものを用意する。JPCERT/CC などの国内組織が公開しているインディケーター情報などを半自動で取得し、一時分析に活用することでモンゴル-日本のインシデント対応における協力を促す。

次に、Public CSIRT Intel Report の作成・公開を行う。これは月次または四半期毎で公開することを想定したインシデント統計のレポートである。Public CSIRT に報告され、ハンドリングを行ったインシデントの件数を、国内・国外や種類（フィッシング、ウェブサイトの侵害、マルウェア、スキャン、DoS、ICS、標的型攻撃等）によって分類した件数を公開する。ここに先述の OSINT で得られたモンゴル国内でのサイバーセキュリティ関連の情報を 5～10 件程度（引用元を明確にしながら公開情報であることが分かるようにして）添えることも望ましい。この Intel Report はその内容そのものにも価値はあるものの、まずは Public CSIRT という組織が存在し、きちんとオペレーションを行っていることを国内外で認知してもらう目的が大きい。

次に、その他の CSIRT、政府機関、民間企業へのリーチを行い、連携を進める。アウトリーチと連携の一環として、セキュアな通信が可能なプライベート SNS、Public CSIRT “HUB” を作成する。ここには Public CSIRT を始め、MNCERT/CC、National CSIRT、軍の CSIRT、サイバーセキュリティベンダー、ISP、その他様々な業種の民間企業のセキュリティ関連部署の職員が参加し、自由に利用することができる。情報共有の範囲は自由に設定でき、また金融部門、地方政府機関、静的マルウェア解析能力を持つチーム、といったようなサブグループを作成できる。Public CSIRT から情報提供することもできるが、それだけでなく、ユーザーにはこの SNS を交流、IoC や検体の共有、その他の情報共有プラットフォームとして利用してもらう。また、年に一回程度、”HUB meet up” 等と称してユーザーを無料で招待する交流会を開催できると好ましい。繰り返しになるが、サイバーセキュリティの情報共有は信頼関係、それも組織間ではなく担当者間レベルでの信

頼関係が無ければ実現しない。

Public CSIRT 内部での連携を手助けする手段として、メッセージプラットフォームも運用する。(名称を仮に“T@LK”とする。)これは Mattermost のようなビジネスチャットのプラットフォームをオンプレミスで導入する。また、ビデオ通話の手段として Microsoft Teams や Cisco Webex 等のアプリケーションを導入できると望ましい。ヒヤリング時点では、Public CSIRT 職員と、コンサルタントとして入っている MNCERT/CC 職員との間のコミュニケーションはメールで行われているということであったが、これも MNCERT/CC 職員が同じメッセージプラットフォームを利用できるようにすることで改善したい。

モンゴル国民へのアウェアネスレイジングの一環として、動画を制作し、YouTube 等の動画 SNS への投稿も行う。これはヒヤリング時に Public CSIRT 職員が希望していた業務の一つであり、また、その必要性が増していることに疑いは無い。JPCERT/CC ではあまり行われてはいないものの、毎年主催するカンファレンス（JSAC）の発表アーカイブを公開する等している。

最後に、CIO 及び CISO のオフィスを設置する。ヒヤリング時に、Public CSIRT 職員には自組織が攻撃の標的となる可能性や、自組織を守る、といった考えが抜け落ちていることに気付いた。そのため、情報管理及びセキュリティの責任者をそれぞれ明確にし、Public CSIRT 自体のシステムの可用性とセキュリティの維持を図る必要がある。

第 4 章：その後の Public CSIRT の経過について(2024 年 9 月時点)

2024 年 9 月 20 日、Public CSIRT と JPCERT/CC で電話会議を実施し、Public CSIRT の活動状況の変化についてヒヤリングを行った。スタッフは 36 名に増加（日本の専門学校の卒業生 2 名が加入した）しており、新しい CEO が就任していた。CEO は MDDC ではなく農水省にあたる省の出身とのことであった。

5 月の訪問以降に始まった活動として、T-POT を設置してのモニタリング（上述の”Eyes”として。まだセンサー数は 1 台であった)、OSINT 業務、アーティファクト分析、113 ホットライン、週次・月次レポートの発行、組織内の情報共有プラットフォームの運用が挙げられた。113 ホットラインは稼働開始後からヒヤリング時点までで約 1,600 件の電話を受け、そのうち約 50 件がサイバー攻撃関係

で、約 130 の IP アドレスの所有者にコンタクトしたとのことであった。また、モンゴルでは救急の電話番号が 103 番であるため、間違い電話も多かった。情報共有プラットフォームについては、T-Guard という複数の情報共有プラットフォームを連結したシステムのインスタンスを設置し、運用を始めているとのことであった。

その他、2025 年に参加予定の国際的なサイバーセキュリティイベントのリストを作成中とのことであったため、JPCERT/CC が毎年 1 月に開催している技術者向けセキュリティカンファレンスの JSAC を紹介した。今後の活動として、翌週から State Digital Service と協力してすべての県を対象にアウェアネス向上のためのトレーニングを実施する予定であることや、オックスフォード大と JICA の協力で翌月からサイバーセキュリティ成熟度アセスメントを実施する計画について共有された。

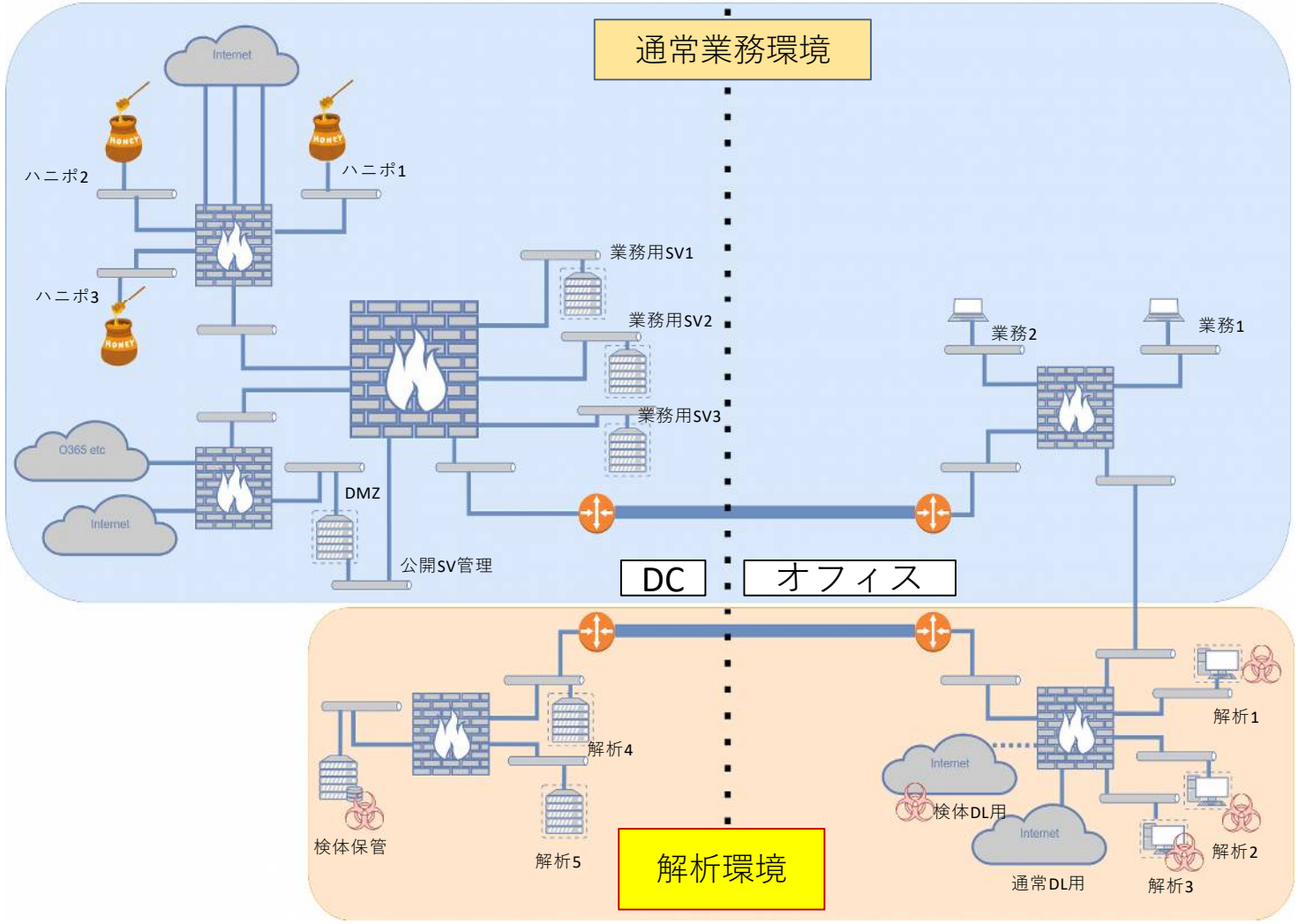
以上の通り、Public CSIRT はまだインシデントレスポンスを行っているオペレーショナルな組織とは言えないものの、組織の第一歩として小規模ながら何らかの活動を始めたことは、前回訪問時からの 4 か月間の成果であると言える。しかしながら、Public CSIRT が国際的にモンゴルのナショナル CERT として認識されるにはまだ遠い。本電話会議の少し前に Google がモンゴルへのサイバー攻撃[1]について発表していたが、本件について Google がコンタクトした先は MNCERT/CC であった。その後、情報が一度 Public CSIRT を経由して、National CSIRT 及び National Data Center に共有されたことも確認しているが、Public CSIRT が間で具体的に何らかの調整を行ったとは思えない。

以上

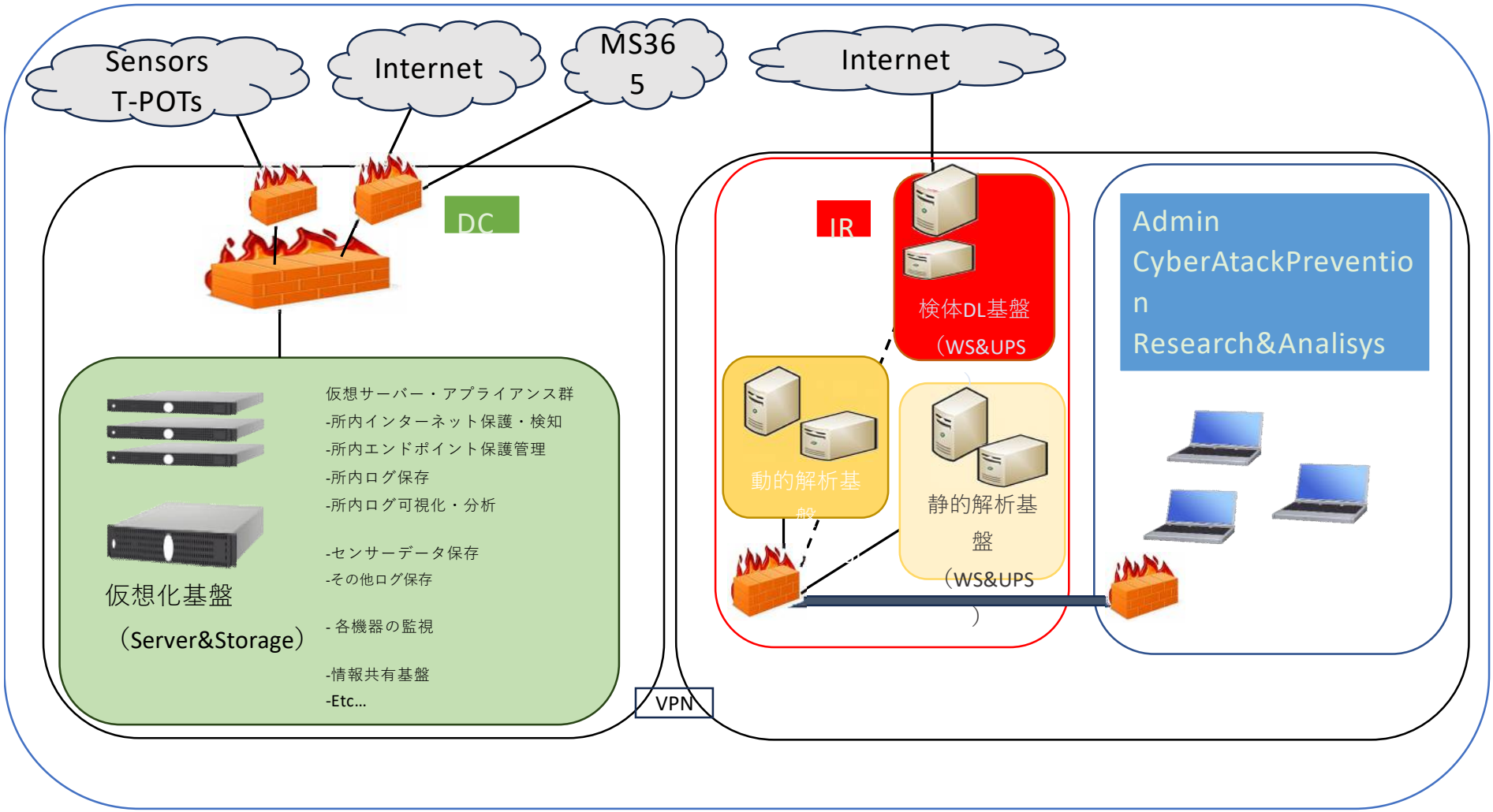
別添資料：提案製品リスト（案）

[1] State-backed attackers and commercial surveillance vendors repeatedly use the same exploits

別添資料：提案製品リスト（案） 概要図



別添資料：提案製品リスト（案） 簡易概要図



別添資料：提案製品リスト（案）（ハードウェア）

番号	種別	用途
1	簡易ラック	NW機器設置用
2	Firewall	DC内セグメンテーション用
3	Firewall	オフィス内セグメンテーション用 IRのオフィスで分析環境用に1セット DCでハニーポット用ルーターとしてそれぞれ使用
4	Firewall	インターネットルーターとして使用
5	NetFlow Collector	
6	AP	オフィス内LAN接続用AP
7	L2スイッチ	オフィス内LAN接続用
8	L2スイッチ	DC内LAN接続用
9	FCスイッチ	DC内FC接続用
10	サーバー	VMのホスト用
11	ストレージ	各種ストレージ用
12	ワークステーション	SOC等業務用
13	ワークステーション	検体解析環境
14	ディスプレイ	業務用
15	UPS	NW機器バックアップ用
16	プロジェクター	ミーティング用
17	スクリーン	ミーティング用
18	生体認証装置	MNCERT居室の隔離用
19	iPadPro	動画編集など
20	カメラ	動画作成用
21	マイク	動画作成用
22	金庫	物理情報保管用
23	テプラPro	ラベリング用
24	シュレッダー	情報の破壊用
25	バックアップアプライアンス	DC内のサーバーのバックアップ
26	内壁	共有スペースと執務室間の自前の仕切り
27	裸族	
28	Webフィルタ&監視	Webフィルタリング
29	Network Sensors	

※保守・ライセンス含む想定
※上記一覧は基礎調査時点での想定

別添資料：提案製品リスト（案）（ソフトウェア及びサービス）

番号	名称	用途
1	T-POT	攻撃情報の収集
2	ELK Stack	収集した情報の可視化
3	Machinarecord	情報を受ける
4	Splunk Enterprise	イベント等のデータの可視化。20GB/Day
5	NetFlow Collector	インターネット接続の出口で、どんな通信が行き来しているのか見るが、CISCOのSW等揃える必要がある。
6	Jira Software	
7	Trellix CTI	
8	Digital Collector	
9	EnCase	
10	Redmine（タスク管理） Apache2（検体の情報管理） MySQL（検体の情報管理） PHP（検体の情報管理）	マルウエア分析情報を共有する
11	Mattermost	
12	VirusTortal	
13	EndpointSecurity EndpointSecurityManagementServer	エンドポイントセキュリティとその管理サーバー
14	Zabbix	機器監視、アラート
15	UTM	動的分析・（一部）静的分析を自動化することによる業務の効率化・省力化
16	JoeSandbox	
17	VMware Workstation Pro	万が一、検体を実行してしまっても問題ないようにリバートできる仮想環境をクローズドNW上で使用している。
18	InetSim(DNS/HTTP(s)/SMTP/POP3/IMAP/NTP…etc) iptables(NAT) FlareVM	マルウエア動的分析環境 検体を実行して動作（発生するトラフィック、レジストリ改変、作成されるファイルなど）を観測する環境。
19	IDA pro(x86/x64/arm…)	検体の解析
20	Almalinux.Ubuntuなど	
21	RegRipper	
22	FTK	
23	Volatility	
24	BurpSuite	
25	Wireshark	
26	Regarding ransomware leak site posts	
27	Write Blocker	
28	checking and evaluation	外部公開サーバーに対する脆弱性診断、ペネトレーションテスト、週一のアドバイザリ
29	AdobeCC	教育用コンテンツの作成
30	Jira Facebook integration	
31	Microsoft 365 Business Basic	Teams
32	Proxy	DCでは通常のインターネット接続用 オフィスの解析部屋では検体のDL、C2サーバーからマルウェア本体のDLにも利用する
33	DCコロケーションサービス	DCでNW機器やサーバー類を設置する
34	法人向けVPN	拠点間接続用
35	VMwareESXiStandard	仮想化基盤。
36	deep analysis	フォレンジックの外部委託
37	RHEL9	
38	WindowsServerSTD 2019	
39	WindowsServer2019 CAL	

※上記一覧は基礎調査時点での想定