トラフィックデータ活用ガイドライン

CES-0160-1

1.0 版：2022 年 10 月 13 日

一般社団法人 情報通信ネットワーク産業協会

目次

目次 1
1. 本ガイドラインの内容 2
2. 参考文献 3
3. 用語定義 4
4. 背景・経緯 5
5. 本ガイドラインの使い方 6
5.1 リファレンスモデル （ステークホルダ、システム構成の定義） 6
6. ガイドライン 7
6.1 ユースケース一覧 7
6.2 ケース 1 セキュリティサービス（分析結果をエンドユーザのみに使用する） 11
6.2.1 ケース 1-1-1 12
6.2.2 ケース 1-1-2 14
6.2.3 ケース 1-2-1 16
6.2.4 ケース 1-2-2 17
6.3 ケース 2 セキュリティサービス
（分析結果をノウハウとして他者のために活用する：追加分） 19
6.4 ケース 3 ネットワーク可視化 21
6.5 ケース 4 端末のネットワーク利用状況の可視化 25
6.5.1 ケース 4-1 26
6.5.2 ケース 4-2 28
6.6 ケース 5 端末の位置情報サービス 29
6.6.1 ケース 5-1-1 30
6.6.2 ケース 5-1-2 32
6.6.3 ケース 5-2-1 33
6.6.4 ケース 5-2-2 34
6.7 項目とユースケースの対応表 35
7. 補足 38
7.1 契約における留意事項 38
7.2 パケットデータの取扱い 40

1. 本ガイドラインの内容

本ガイドラインは、企業内ネットワークトラフィックデータの活用において、対象サービスを提供するベンダー／サービス事業者、サービスを受けるユーザが、検討すべき項目を提供する。対象とする企業内ネットワークは電気通信事業法の範囲外であることを補足しておく。

これにより、上記ベンダー／サービス事業者、ユーザが安心して、サービスを提供、享受できる環境の構築に貢献し、市場の活性化を期待するものである。

以下、トラフィックデータ活用の具体的ユースケースを示し、ベンダー／サービス事業者／ユーザそれぞれの立場にて、検討すべき項目を示す。

2. 参考文献

表 2-1

NO.	文献名	補足
1	AI・データの利用に関する契約ガイドライン	https://www.meti.go.jp/press/2019/12/20191209001/20191209001.html （2019 年 12 月）
2	カメラ画像利活用ガイドブック	https://www.soumu.go.jp/main_content/000542668.pdf （2018 年 3 月）
3	IoT セキュリティガイドライン	https://www.soumu.go.jp/main_content/000428393.pdf （2016 年 7 月）
4	データ利活用のてびき	https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/datatebiki.pdf （2020 年 6 月）
5	新たなデータ流通取引に関する検討事例集	https://www.soumu.go.jp/main_content/000568809.pdf （2018 年 8 月）
6	電気通信事業法	https://elaws.e-gov.go.jp/document?lawid=359AC0000000086 （2021 年 7 月）

3. 用語定義

表 3-1

NO.	用語	本ガイドブックにおける定義
1	プローブ装置	ネットワーク上の特定位置に設置し、パケットを探針することを目的とした装置。
2	TAP 装置	ネットワーク上の特定位置に設置し、パケットを探針することを目的とした装置であり、上記プローブ装置に対して低レイヤにてパケットデータを取り出す装置。 （例：光伝送における光スプリット装置など）

4. 背景・経緯

ネットワーク上を流れるトラフィックデータを分析することで、システム運用の省力化、インフラシステムの最適化、サイバーセキュリティ対策など様々な活用が期待される。

たとえば、異常或いは不正なトラフィックを検出することでサイバー攻撃を検出し適切な対処を施す、トラフィックの変化を検出してネットワークの強化を提案する、ネットワーク障害時にトラフィックを観測し障害箇所、原因を早期に特定し適切な対処を行うなどがある。

一方、あらゆる情報がネットワーク上でやりとりされる状況下で、これらのデータ収集については、プライバシーや企業秘密の保護について、社会的な懸念が論じられることも多い。トラフィックデータの観測時に、同時に企業秘密がのぞき見されることや、データに含まれるプライバシー情報を抽出される懸念が挙げられる。

さらに、個人情報保護法、GDPR、不正競争防止法といった、新たな社会規範が策定されており、これらに見合う対応が必要となっている。

以上のことから、ベンダー／サービス事業者／ユーザそれぞれの立場にて、検討すべき項目を示すことで、安心してサービスを提供、享受できる環境の構築に貢献し、トラフィックデータ活用市場が活性化することを期待したい。

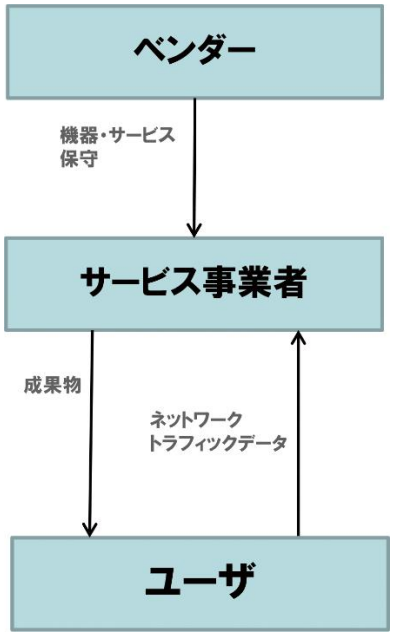
5. 本ガイドラインの使い方

表 5-1

対象者	本ガイドラインの 活用タイミング	本ガイドラインの 活用メリット
ベンダー	・対象となる機器／サービスの設計段階。	・機器／サービスの品質向上。
サービス事業者	・ベンダー／機器／サービスの選定検討段階。 ・ベンダーとの契約段階。	・サービスの品質向上。 ・ベンダーとの契約締結の効率化。 ・訴訟等に繋がる事案時に不利にならない。
	・サービス／製品の構築検討段階。	・サービスの品質向上。
	・ユーザとの契約段階。	・ユーザとの契約締結の効率化。 ・訴訟等に繋がる事案時に不利にならない。
ユーザ	・サービス事業者／サービスの選定検討段階。 ・サービス事業者との契約段階。	・サービス導入の効率化。 ・サービス事業者との契約締結の効率化。 ・訴訟等に繋がる事案時に不利にならない。

5.1 リファレンスモデル （ステークホルダ、システム構成の定義）

表 5-2

ステークホルダ	定義	システム構成上の位置付け
ベンダー	ネットワーク上のトラフィックデータを活用するサービスにおいて、それを構成する、機器、サービス、保守を提供する。	
サービス事業者	上記ベンダーから提供される、機器、サービス、保守をサービス事業として構成する。ユーザからのトラフィックデータを収集／加工し、成果物（分析結果等）を提供する。 ベンダーと兼ねるケースもある。	
ユーザ	サービス事業者に対しトラフィックデータを提供し、成果物を受け取る。 ユーザネットワークは、ユーザが所有する。	

6. ガイドライン

6.1 ユースケース一覧

表 6-1

ケース番号	サービス名	概要
1	セキュリティサービス（分析結果をエンドユーザのみに使用する）	トラフィックデータを分析して、サイバー攻撃を検知し、通知を行うサービス。収集したデータの分析結果は、収集元企業へのサービスのみに利用される。
2	セキュリティサービス（分析結果をノウハウとして他者のために活用する：追加分）	複数の異なる企業からトラフィックデータを収集し、分析結果としてのノウハウを蓄積。ノウハウは、他の顧客にも適用可。同業他社に提供可。
3	ネットワーク可視化	・設備障害対応の迅速化、自動化。 ・運用容易化。 ・インフラ UX 向上。 ・設備最適化コンサル。
4	端末のネットワーク利用状況の可視化	・業務アプリケーションの利用可視化。 ・従業員の業務分析。
5	端末の位置情報サービス	・顧客動線の可視化、行動分析。 ・従業員動線の可視化、行動分析。

ケース 1 セキュリティサービス（分析結果をエンドユーザのみに使用する）

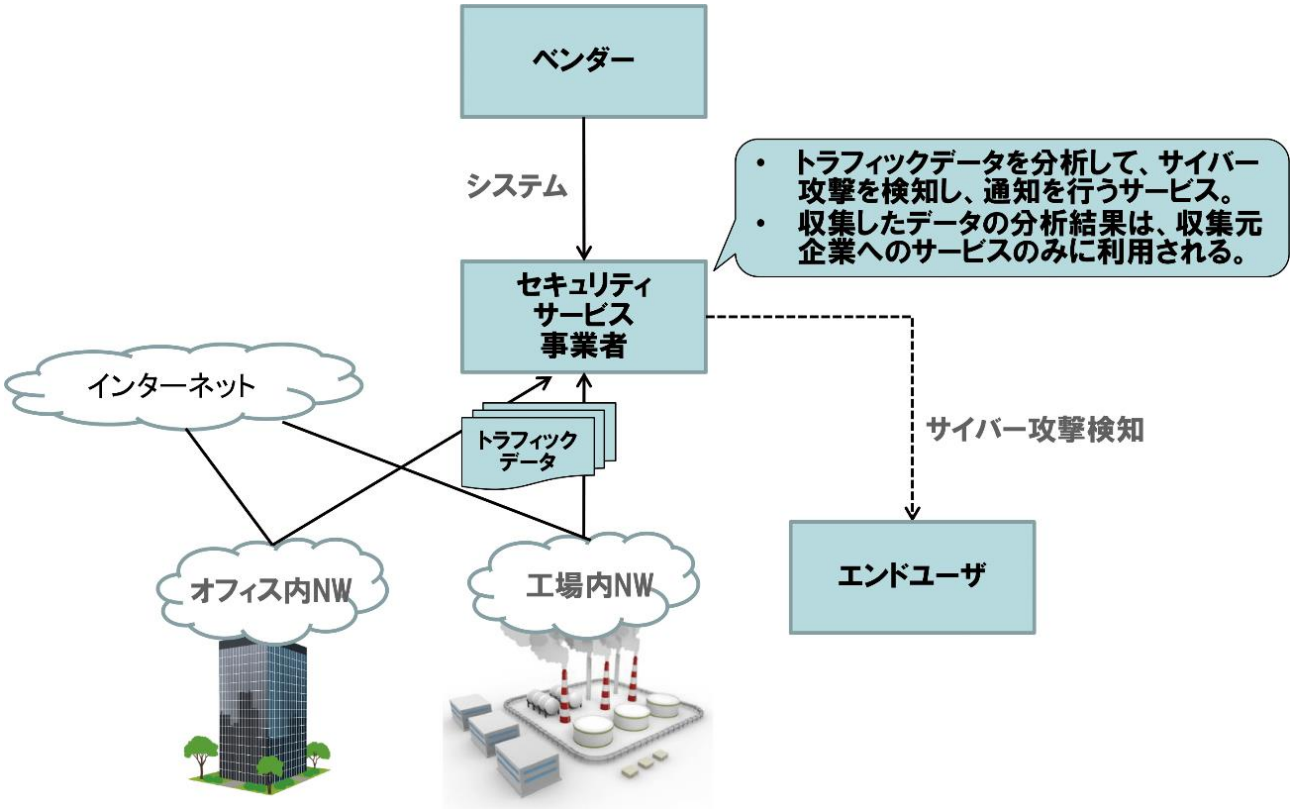


図 6-1

ケース 2 セキュリティサービス（分析結果をノウハウとして他者のために活用する：追加分）

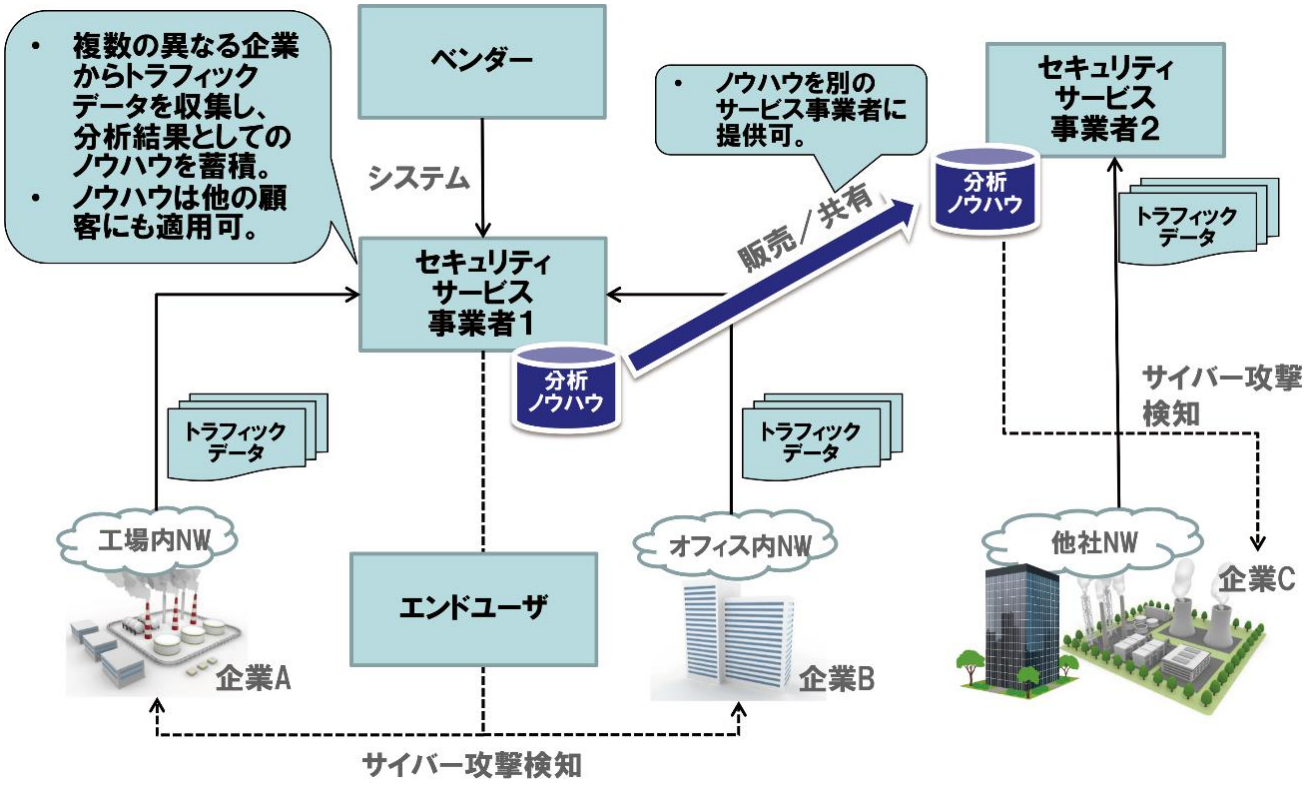


図 6-2

ケース 3 ネットワーク可視化

- 設備障害対応の迅速化、自動化。
- 運用容易化。
- インフラ UX 向上。
- 設備最適化コンサル。

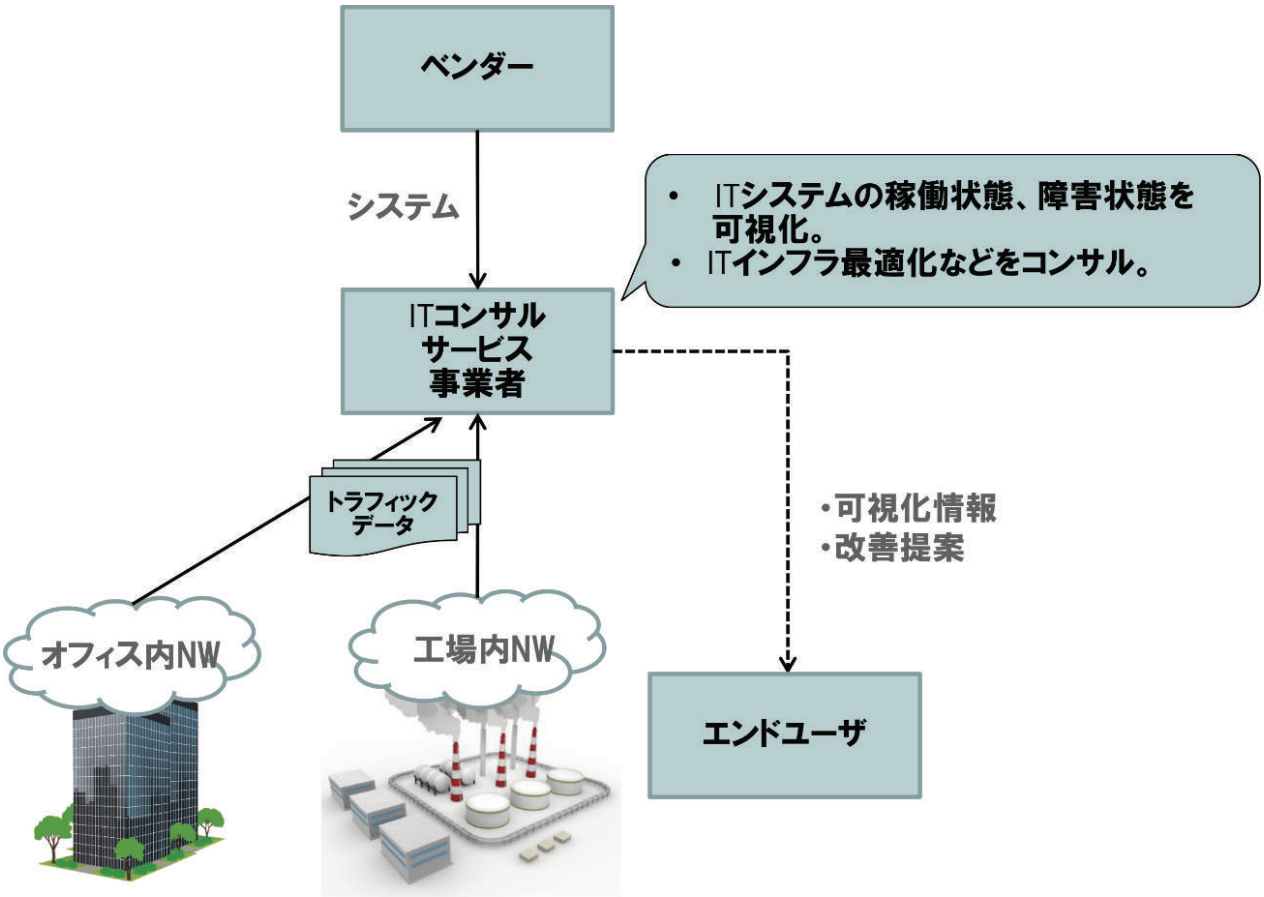


図 6-3

ケース 4 端末のネットワーク利用状況の可視化

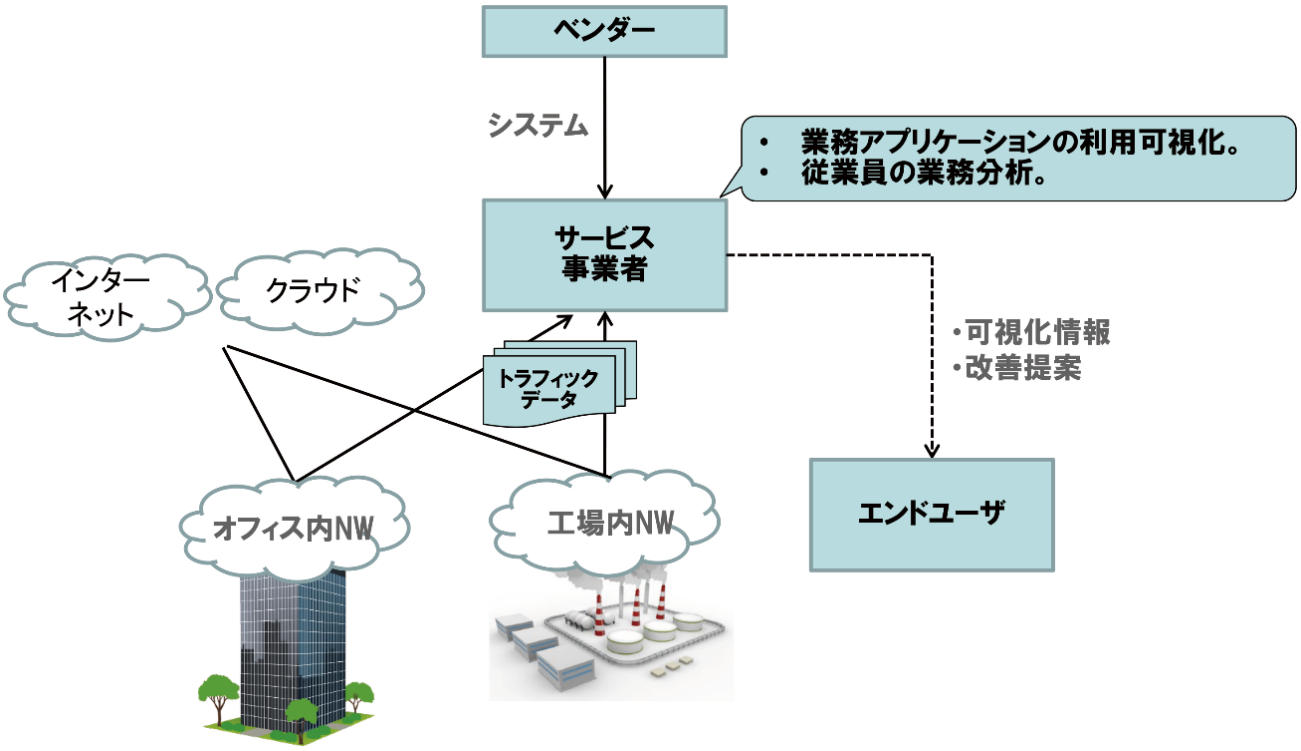


図 6-4

ケース 5 端末の位置情報サービス

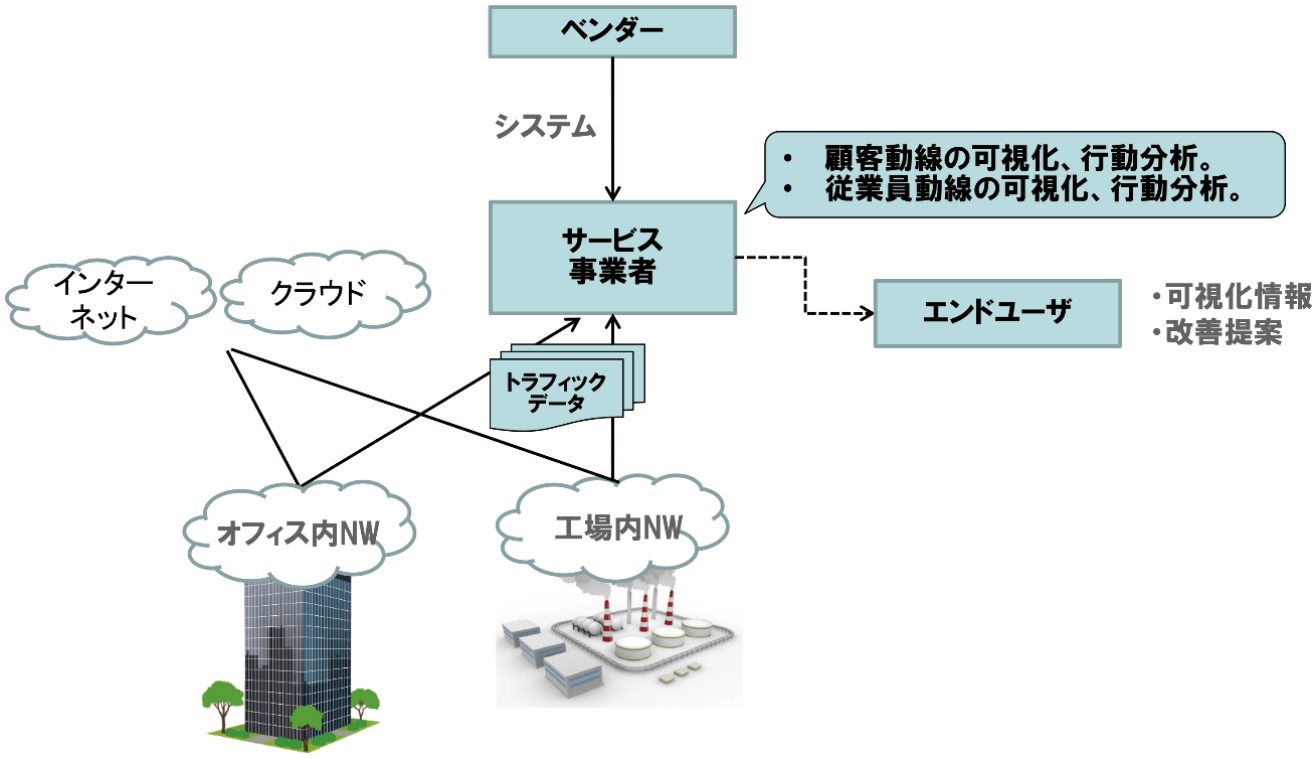


図 6-5

6.2 ケース 1 セキュリティサービス（分析結果をエンドユーザのみに使用する）

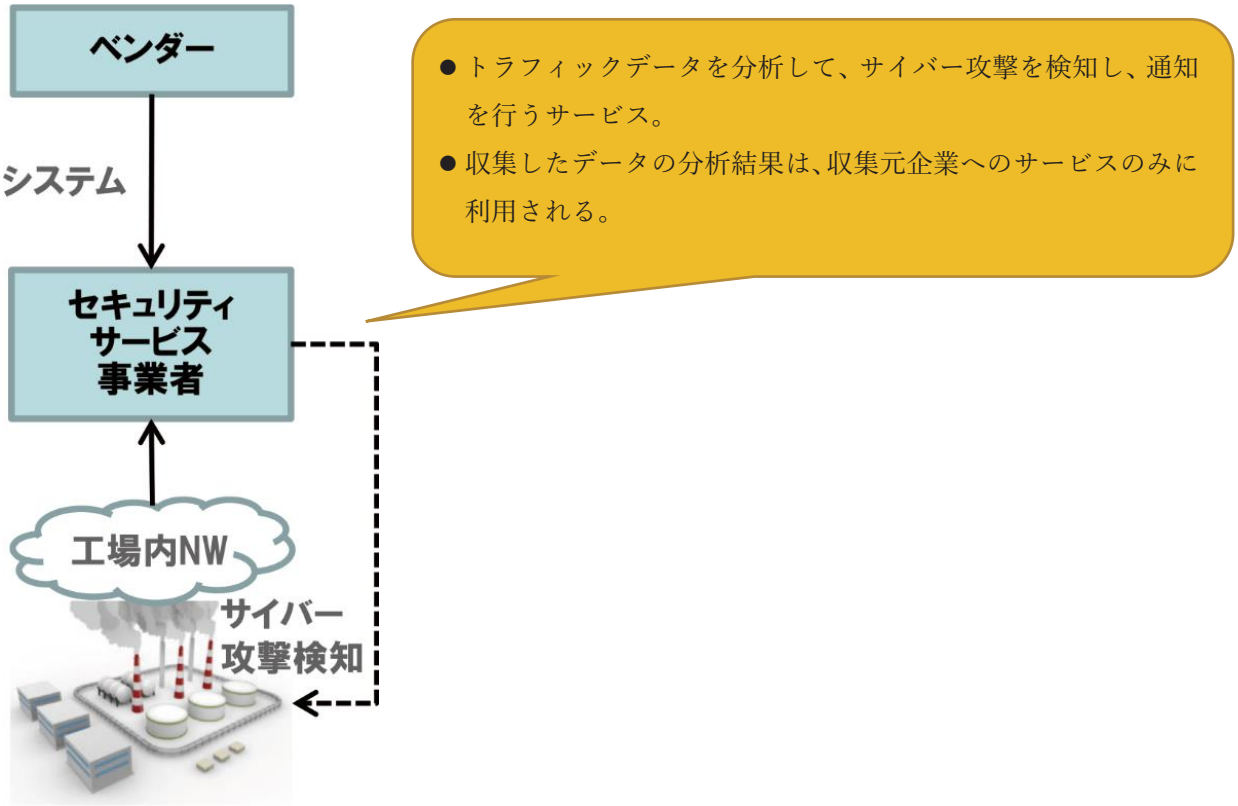


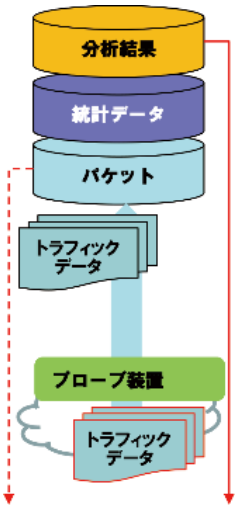
図 6-6

表 6-2

	ケース 1-1-1	ケース 1-1-2	ケース 1-2-1	ケース 1-2-2
セキュリティサービス事業者 エンドユーザ	分析結果 統計データ パケット トラフィックデータ プローブ装置 トラフィックデータ	分析結果 統計データ パケット トラフィックデータ パケット プローブ装置 トラフィックデータ	分析結果 統計データ 統計データ パケット プローブ装置 トラフィックデータ	分析結果 統計データ 統計データ プローブ装置 トラフィックデータ
	トラフィックデータをそのまま上げて分析。パケット提供有／無の両ケースあり。	パケットデータを上げるが、プローブ装置にも提供用に保存。	統計データのみを上げ、プローブ装置には提供用にパケットデータを保持。	統計データのみを上げ、パケットデータ提供は無し。

6.2.1 ケース 1-1-1

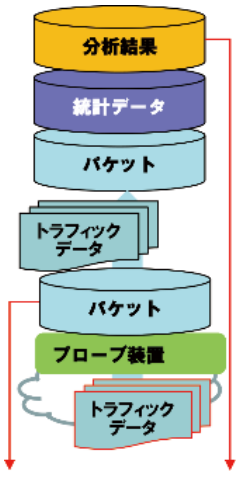
表 6-3

	ケース 1-1-1	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いをどうすればいいのか？	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	契約／運用
				解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	
				消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	
			（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	契約／運用
				上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	
セキュリティサービス事業者		データの扱い	（1）パケットの PDU 部分にエンドユーザの機密情報などが含まれる可能性があるが、漏洩防止など、どこまでやれば良いのかがわからない。	受領するパケットデータについて、利用目的（セキュリティ分析）、利用者（サービス事業者＋エンドユーザ）、取扱いなどを規定した NDA 条項を契約する。	契約／運用
			（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	運用
		システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	運用
		データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	契約／運用
		権利関連	（5）分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、所有権、活用内容、その可否について合意し契約として締結しておくこと。 補足 7.1 を参照。。	契約／運用
エンドユーザ		データの扱い	（1）プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。	プローブ内の保管データ／保管期間、送信データなどがサービス仕様内に規定しているか確認し、その内容を確認すること。	運用
			（2）トラフィックデータの PDU に含まれる企業機密・個人情報は ①データとして取り出されるのだろうか？ ②サービス事業者で適切にアクセス管理されるのだろうか？	契約で規定。（上記サービス事業者（1）を参照）	契約／運用

	ケース 1-1-1	課題分類	課題／心配事	対応策	対応分類
			（3）個人情報を意図せずサービス事業者に渡していないだろうか？	事業者が提示するサービス仕様から、送信されるパケットデータ種別を確認する。パケットデータから個人情報を復元できる場合は、個人情報を渡しているとみなされ得るので、適切な扱いが必要。（詳細は個人情報保護法を参照） 日本では MAC アドレス単体では個人識別性を有しないが、他の情報と容易に照合できる場合は個人識別性をもつ。MAC アドレスとユーザを結び付ける情報の提示有無を確認すること。	法令
			（4）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	契約／運用
			（5）異常を検知した際に、該当するパケットデータも送られてくるのはいいが、その PDU に含まれる企業機密／個人情報の管理が難しい。（オリジナルの情報であれば社内のルールに従って管理される）	（ポイント）まずはデータが返送されるサービスの有無の確認。ある場合、自社データではあるが、管理部署とは違う部署にデータが送られる場合、管理上問題になるか否か事前に確認しておくこと。 別途、受領パケットデータの取扱いについて規定が必要。	運用
			（6）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要になるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	運用
		システム設計	（7）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検討すること。	契約／運用
			（8）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	契約／運用
		データの扱い	（9）エンドユーザ NM 内の利用者（エンドユーザ内の従業員）への告知。	従業員からの同意取得について、新たなデータ流通取引に関する検討事例集 ver2.0<検討事例 1-05>を参考。	運用
			（10）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	契約／運用
		システム設計	（11）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（7）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	契約／運用
			（12）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	契約
説明	トラフィックデータをそのまま上げて分析。パケット提供有／無の両ケースあり。				

6.2.2 ケース 1-1-2

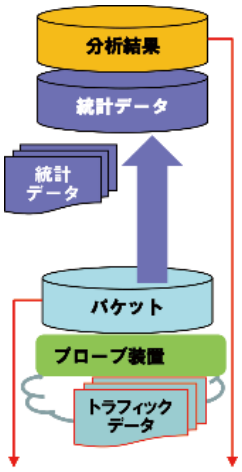
表 6-4

	ケース 1-1-2	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いをどうすればいいのか？	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	契約／運用
				解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	
				消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	
			（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	契約／運用
				上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	
			（3）プローブ装置に不正にログインされた場合、パケット格納装置内データが盗みとられないか？	多段認証など、不正ログインへの対策と合わせて、パケット格納装置内データへのアクセスセキュリテイを、装置ログインとは別に設けるなど、検討する。	運用のみ
		システム障害	（4）故障発生時にパケット格納装置が返送された際、格納されたデータの取扱いをどうすればいいのか？	ケース 1-1-1 と同じく、返却前にパケット格納装置内のデータを全消去して送付する旨を、マニュアル等記載し、事前に周知しておく。	契約／運用
セキュリティサービス事業者		データの扱い	（1）パケットの PDU 部分にエンドユーザの機密情報などが含まれる可能性があるが、漏洩防止など、どこまでやれば良いのかがわからない。	受領するパケットデータについて、利用目的（セキュリティ分析）、利用者（サービス事業者＋エンドユーザ）、取扱いなどを規定した NDA 条項を契約する。	契約／運用
			（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	運用
		システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	運用
		データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	契約／運用
		権利関連	（5）分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、所有権、活用内容、その可否について合意し契約として締結しておくこと。 補足 7.1 を参照。。	契約／運用
エンドユーザ		データの扱い	（1）プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。	プローブ内の保管データ／保管期間、送信データなどがサービス仕様内に規定しているか確認し、その内容を確認すること。	運用
			（2）トラフィックデータの PDU に含まれる企業機密・個人情報は ①データとして取り出されるのだろうか？ ②サービス事業者で適切にアクセス管理されるのだろうか？	契約で規定。（上記サービス事業者（1）を参照）	契約／運用

	ケース 1-1-2	課題分類	課題／心配事	対応策	対応分類
			（3）個人情報を意図せずサービス事業者に渡していないだろうか？	事業者が提示するサービス仕様から、送信されるパケットデータ種別を確認する。パケットデータから個人情報を復元できる場合は、個人情報を渡しているとみなされ得るので、適切な扱いが必要。（詳細は個人情報保護法を参照） 日本では MAC アドレス単体では個人識別性を有しないが、他の情報と容易に照合できる場合は個人識別性をもつ。MAC アドレスとユーザを結び付ける情報の提示有無を確認すること。	法令
			（4）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	契約／運用
			（5）異常を検知した際に、該当するパケットデータも送られてくるのはいいが、その PDU に含まれる企業機密／個人情報の管理が難しい。（オリジナルの情報であれば社内のルールに従って管理される）	（ポイント）まずはデータが返送されるサービスの有無の確認。ある場合、自社データではあるが、管理部署とは違う部署にデータが送られる場合、管理上問題になるか否か事前に確認しておくこと。 別途、受領パケットデータの取扱いについて規定が必要。	運用
			（6）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要になるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	運用
		システム設計	（7）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検討すること。	契約／運用
			（8）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	契約／運用
		データの扱い	（9）エンドユーザ NM 内の利用者（エンドユーザ内の従業員）への告知。	従業員からの同意取得について、新たなデータ流通取引に関する検討事例集 ver2.0<検討事例 1-05>を参考。	運用
			（10）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	契約／運用
		システム設計	（11）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（7）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	契約／運用
			（12）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	契約
説明	パケットデータを上げるが、プローブ装置にも提供用に保存。				

6.2.3 ケース 1-2-1

表 6-5

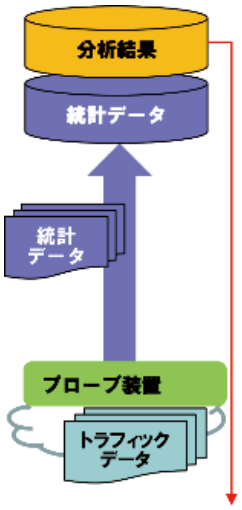
	ケース 1-2-1	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いをどうすればいいのか？	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	契約／運用
				解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	
				消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	
			（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	契約／運用
				上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	
			（3）プローブ装置に不正にログインされた場合、パケット格納装置内データが盗みとられないか？	多段認証など、不正ログインへの対策と合わせて、パケット格納装置内データへのアクセスセキュリテイを、装置ログインとは別に設けるなど、検討する。	運用のみ
		システム障害	（4）故障発生時にパケット格納装置が返送された際、格納されたデータの取扱いをどうすればいいのか？	ケース 1-1-1 と同じく、返却前にパケット格納装置内のデータを全消去して送付する旨を、マニュアル等記載し、事前に周知しておく。	契約／運用
セキュリティサービス事業者		データの扱い	（1）パケットの PDU 部分にエンドユーザの機密情報などが含まれる可能性があるが、漏洩防止など、どこまでやれば良いのかがわからない。	受領するパケットデータについて、利用目的（セキュリティ分析）、利用者（サービス事業者＋エンドユーザ）、取扱いなどを規定した NDA 条項を契約する。	契約／運用
			（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	運用
		システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	運用
		データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	契約／運用
		権利関連	（5）分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、所有権、活用内容、その可否について合意し契約として締結しておくこと。 補足 7.1 を参照。。	契約／運用
エンド		データの扱い	（1）プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。	プローブ内の保管データ／保管期間、送信データなどがサービス仕様内に規定しているか確認し、その内容を確認すること。	運用

	ケース 1-2-1	課題分類	課題／心配事	対応策	対応分類
			（2）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	契約／運用
			（3）異常を検知した際に、該当するパケットデータも送られてくるのはいいが、その PDU に含まれる企業機密／個人情報の管理が難しい（オリジナルの情報であれば社内のルールに従って管理される）	（ポイント）まずはデータが返送されるサービスの有無の確認。ある場合、自社データではあるが、管理部署とは違う部署にデータが送られる場合、管理上問題になるか否か事前に確認しておくこと。 別途、受領パケットデータの取扱いについて規定が必要。	運用
			（4）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要になるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	運用
		システム設計	（5）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検討すること。	契約／運用
			（6）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	契約／運用
		データの扱い	（7）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	契約／運用
		システム設計	（8）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（7）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	契約／運用
			（9）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	契約
説明	統計データのみを上げ、プローブ装置には提供用にパケットデータを保持。				

6.2.4 ケース 1-2-2

表 6-6

	ケース 1-2-2	課題分類	課題／心配事	対応策	対応分類
ベン		システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いを	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	契約／運用

	ケース 1-2-2	課題分類	課題／心配事	対応策	対応分類
			どうすればいいのか？	解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	
				消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	
			（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	契約／運用
				上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	
セキュリティサービス事業者		データの扱い	（1）パケットの PDU 部分にエンドユーザの機密情報などが含まれる可能性があるが、漏洩防止など、どこまでやれば良いのかがわからない。	受領するパケットデータについて、利用目的（セキュリティ分析）、利用者（サービス事業者＋エンドユーザ）、取扱いなどを規定した NDA 条項を契約する。	契約／運用
			（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	運用
		システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	運用
		データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	契約／運用
		権利関連	（5）分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、所有権、活用内容、その可否について合意し契約として締結しておくこと。 補足 7.1 を参照。。	契約／運用
エンドユーザ		データの扱い	（1）プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。	プローブ内の保管データ／保管期間、送信データなどがサービス仕様内に規定しているか確認し、その内容を確認すること。	運用
			（2）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	契約／運用
			（3）異常を検知した際に、該当するパケットデータも送られてくるのはいいが、その PDU に含まれる企業機密／個人情報の管理が難しい（オリジナルの情報であれば社内のルールに従って管理される）	（ポイント）まずはデータが返送されるサービスの有無の確認。ある場合、自社データではあるが、管理部署とは違う部署にデータが送られる場合、管理上問題になるか否か事前に確認しておくこと。 別途、受領パケットデータの取扱いについて規定が必要。	運用
			（4）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要になるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	運用
		システム設計	（5）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検	契約／運用

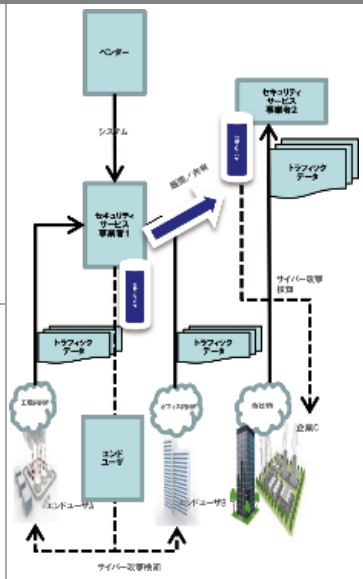
	ケース 1-2-2	課題分類	課題／心配事	対応策	対応分類
				討すること。	
			（6）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	契約／運用
		データの扱い	（7）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	契約／運用
		システム設計	（8）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（7）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	契約／運用
			（9）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	契約
説明	統計データのみを上げ、パケットデータ提供は無し。				

6.3 ケース 2 セキュリティサービス（分析結果をノウハウとして他者のために活用する：追加分）

基本はケース 1 に従う。他者利用をする場合のポイントを示す。

表 6-7

	ケース 2	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム設計	セキュリティサービス事業者に分析ノウハウを収集、移転、など活用するための機能、運用。	データを匿名化したり、ノウハウだけを取り出す機能を提供する。特にプライバシーについては、問題ないことを明示できるチェック機能が提供する。	契約／運用
セキュリティサービス事業者		データの扱い	分析ノウハウの販売／共有に関する注意、取扱い方法や通信の秘密や個人情報保護法などの法的問題に気を付ける必要がある。	データ販売か、ノウハウだとどんな権利やサービスになるのかをはっきりさせて対処する。特に法的な扱いがかわる可能性があるため、契約内容と運用方法について整理する。	契約／運用
		システム設計	複数のユーザから取得したデータをまとめて扱うことに関する注意。 元はどこのデータなのかをデバッグなどのために追従できる方法とプライバシーなどを考慮してわからないようにして、ノウ	権利関係を整理するとともに、運用と管理のための困らないような対応ができるようにしておく。 アクセスレベルを設定・誠意減し、データをそのまま／難読化／統計処理の 3 つのレベルのいずれを選択し、対応する。	契約／運用

	ケース 2	課題分類	課題／心配事	対応策	対応分類
			ハウだけを何らかの方法で受け渡す。		
		権利関連	ノウハウはデータとして受け渡すが、データの内容の権利や帰属とノウハウの帰属の整理。	契約事項として、利用条件、活用内容、その可否について合意し契約として締結しておくこと。	契約／運用
エンドユーザ		権利関連	データ取得や仕様、加工データの権利とその帰属。	ユーザから利用許諾をとる。その中で利用条件、活用内容、その可否について明記する。	契約／運用
説明	基本は「ケース 1」でここには追加分だけを示す。				

6.4 ケース 3 ネットワーク可視化

- 設備障害対応の迅速化、自動化。
- 運用容易化。
- インフラ UX 向上。
- 設備最適化コンサル

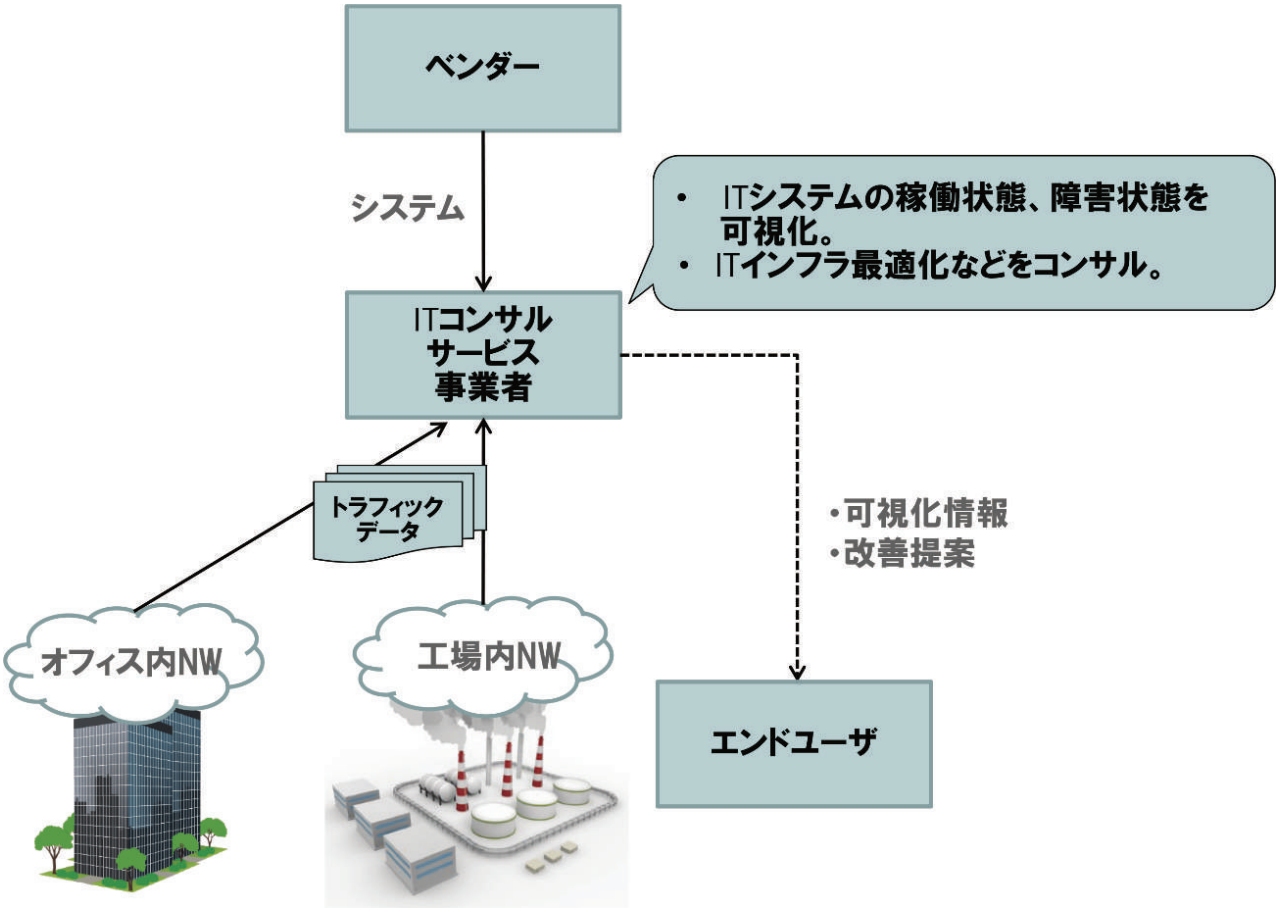
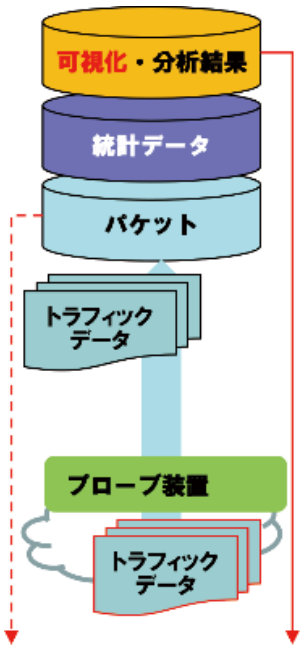


図 6-7

表 6-8

	ケース 3	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いをどうすればいいのか？	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	契約／運用
				解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	
				消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	

	ケース 3	課題分類	課題／心配事	対応策	対応分類
			（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	契約／運用
				上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	
			（3）収集データの格納領域の確保について。	データ量予測や容量設計機能・通知機能等が求められる。また、大量データの転送機能についても考慮が必要。	設計／構築
			（4）可視化結果データの参照のレベル分け機能。	可視化データの参照内容を参照者によってレベル分けできる機能を IT コンサルサービス事業者と相談しながら具備しておくこと。	設計／構築
ITコンサルサービス事業者		データの扱い	（1）パケットの PDU 部分にエンドユーザの機密情報などが含まれる可能性があるが、漏洩防止など、どこまでやれば良いのかがわからない。	受領するパケットデータについて、利用目的（セキュリティ分析）、利用者（サービス事業者＋エンドユーザ）、取扱いなどを規定した NDA 条項を契約する。	契約／運用
			（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	運用
		システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	運用
		データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	契約／運用
			（5）参照可能とする可視化データの対象期間・種別等の明確化。	一般的にネットワーク可視化に必要とされるデータは大量となるため、過去データの保管期間や、過去データの表示種別等について仕様の明確化が求められる。	設計／構築
			（6）可視化結果の参照権のレベル分け。 ・運用者とエンドユーザ。 ・ユーザ内。（一般ユーザ、管理職等の特権ユーザ） ・ユーザ単位。（当事者企業、参照可能な会員企業）	可視化結果のレベル分けと各々の参照権について、設計時よりサービス仕様を明確化し、ベンダー装置の機能が要件を満たしているかどうかの確認を行うと共に、及びレベル分けの単位やサービス価格等についてエンドユーザとの合意を取ること。	設計／構築
		権利関連	（7）可視化のための分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、利用条件、活用内容、その可否について合意し契約として締結しておくこと。	契約／運用
			（8）可視化した結果そのもの、または結果を一部加工したものを、他のサービスへ利用可能か、事前に合意しておくこと。	契約事項として、利用条件、活用内容、その可否について合意し契約として締結しておくこと。	契約／運用

	ケース 3	課題分類	課題／心配事	対応策	対応分類
			（9）可視化した結果や結果を一部加工した内容を、他の有償サービス提供顧客から参照可能とできるか、事前に合意しておくこと。	契約事項として、結果の第三者の参照可否、参照条件等について合意し契約として締結しておくこと。	契約／運用
エンドユーザ		データの扱い	（1）プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。	プローブ内の保管データ／保管期間、送信データなどがサービス仕様内に規定しているか確認し、その内容を確認すること。	運用
			（2）トラフィックデータの PDU に含まれる企業機密・個人情報は ①データとして取り出されるのだろうか？ ②サービス事業者で適切にアクセス管理されるのだろうか？	契約で規定。（上記サービス事業者（1）を参照）	契約／運用
			（3）個人情報を意図せずサービス事業者に渡していないだろうか？	事業者が提示するサービス仕様から、送信されるパケットデータ種別を確認する。パケットデータから個人情報を復元できる場合は、個人情報を渡しているとみなされ得るので、適切な扱いが必要。（詳細は個人情報保護法を参照） 日本では MAC アドレス単体では個人識別性を有しないが、他の情報と容易に照合できる場合は個人識別性をもつ。MAC アドレスとユーザを結び付ける情報を提示有無を確認すること。	法令
			（4）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	契約／運用
			（5）サービス事業者が当社の可視化結果を、当社への利益供与を行う前提で、他社へサービスを行うことはできるか。	サービス事業者の間で、可視化結果の共有範囲、第三者へ結果の参照を認める場合の当社への対価等を契約内で規定する必要がある。	契約／運用
			（6）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要なるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	運用
		システム設計	（7）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検討すること。	契約／運用
			（8）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	契約／運用
		データの扱い	（9）エンドユーザ NM 内の利用者（エンドユーザ内の従業員）への告知。	従業員からの同意取得について、新たなデータ流通取引に関する検討事例集 ver2.0<検討事例 1-05>を参考。	運用
			（10）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	契約／運用

	ケース 3	課題分類	課題／心配事	対応策	対応分類
		システム設計	（11）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（7）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	契約／運用
			（12）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	契約
説明	トラフィックデータをそのまま上げて分析。パケット提供有／無の両ケースあり。				

6.5 ケース 4 端末のネットワーク利用状況の可視化

暗号化通信もエンドユーザの協力があれば、鍵を指定して復号可能。ただし、ネットワーク利用状況の可視化サービスがこのような復号を行うケースは一般的では無いと考え、本ケースでは復号しない場合についてのみ述べる。

（複合する場合、ペイロード部分を解析して利用ユーザ ID を特定するといった分析も考えられる）

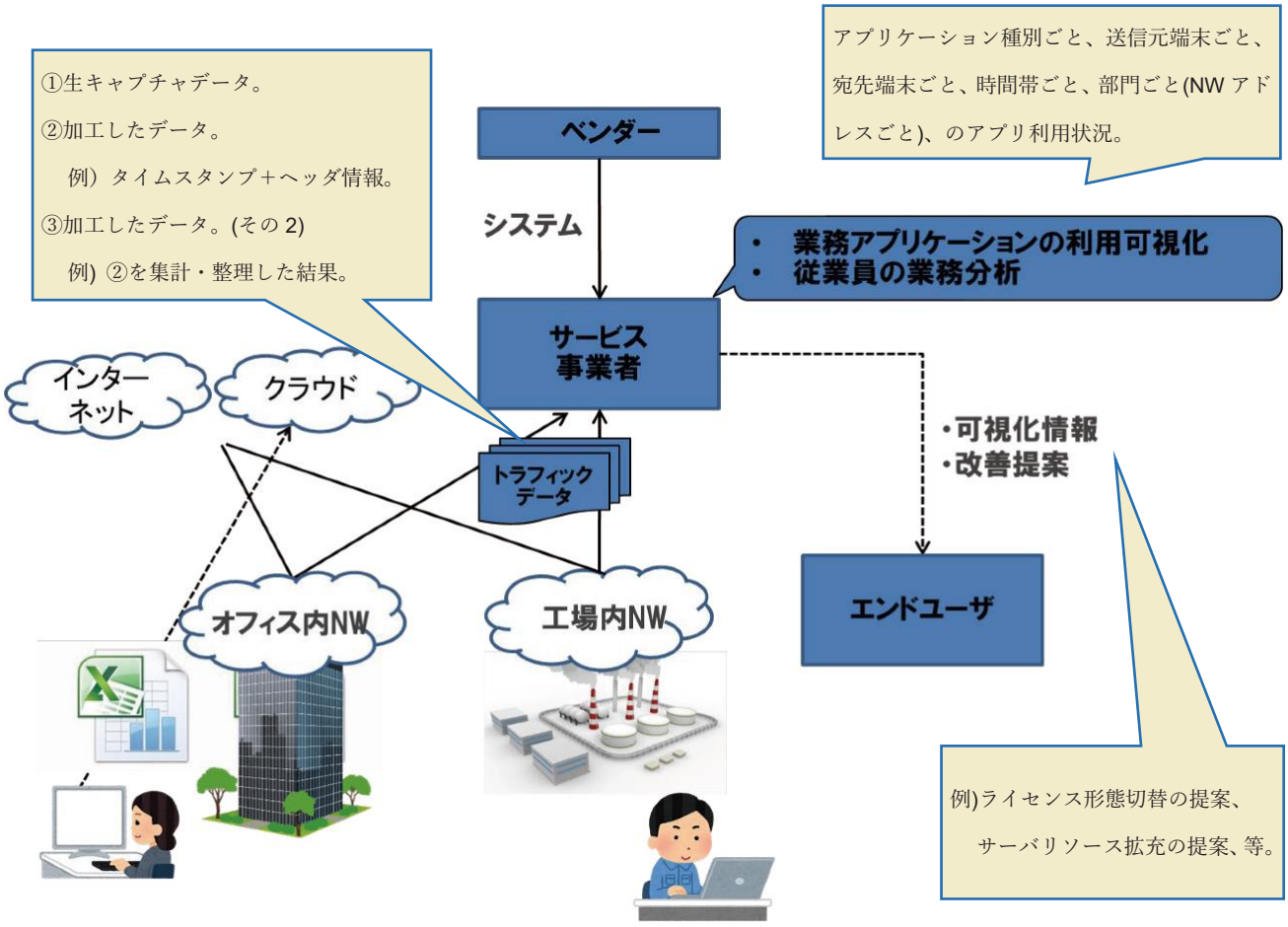


図 6-8

トラフィックデータが①②③のいずれであったとしても、
プローブ装置に生キャプチャデータを溜め込む必要は無いと考える。

6.5.1 ケース 4-1

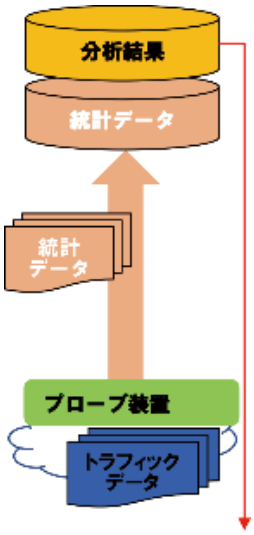
表 6-9

	ケース 4-1	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いをどうすればいいのか？	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	契約／運用
				解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	
				消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	
			（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	契約／運用
				上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	
セキュリティサービス事業者	分析結果 統計データ パケット トラフィックデータ プローブ装置 トラフィックデータ	データの扱い	（1）パケットの PDU 部分にエンドユーザの機密情報などが含まれる可能性があるが、漏洩防止など、どこまでやれば良いのかがわからない。	受領するパケットデータについて、利用目的（セキュリティ分析）、利用者（サービス事業者＋エンドユーザ）、取扱いなどを規定した NDA 条項を契約する。	契約／運用
			（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	運用
		システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	運用
		データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	契約／運用
		権利関連	（5）分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、所有権、活用内容、その可否について合意し契約として締結しておくこと。 補足 7.1 を参照。。	契約／運用
エンドユーザ		データの扱い	（1）プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。	プローブ内の保管データ／保管期間、送信データなどがサービス仕様内に規定しているか確認し、その内容を確認すること。	運用
			（2）トラフィックデータの PDU に含まれる企業機密・個人情報は ①データとして取り出されるのだろうか？ ②サービス事業者で適切にアクセス管理されるのだろうか？	契約で規定。（上記サービス事業者（1）を参照）	契約／運用
			（3）個人情報を意図せずサービス事業者に渡していないだろうか？	事業者が提示するサービス仕様から、送信されるパケットデータ種別を確認する。パケットデータから個人情報を復元できる場合は、個人情報を渡しているとみなされ得るので、適切な扱いが必要。（詳細は個人情報保護法を参照） 日本では MAC アドレス単体では個人識別性を有しないが、他の情報と容易に照合できる場合は個人識別性をもつ。MAC アドレスとユーザを結び付ける情報を提示有無を確認すること。	法令

	ケース 4-1	課題分類	課題／心配事	対応策	対応分類
			（4）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	契約／運用
			（6）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要なるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	運用
		システム設計	（7）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検討すること。	契約／運用
			（8）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	契約／運用
		データの扱い	（9）エンドユーザ NM 内の利用者（エンドユーザ内の従業員）への告知。	従業員からの同意取得について、新たなデータ流通取引に関する検討事例集 ver2.0<検討事例 1-05>を参考。	運用
			（10）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	契約／運用
		システム設計	（11）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（7）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	契約／運用
			（12）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	契約
説明	トラフィックデータをそのまま上げて分析。パケットデータのプローブ装置内での蓄積や、パケットデータのエンドユーザへの提供は無し。				

6.5.2 ケース 4-2

表 6-10

	ケース 4-2	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いをどうすればいいのか？	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	契約／運用
				解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	
				消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	
			（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	契約／運用
				上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	
セキュリティサービス事業者		データの扱い	（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	運用
		システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	運用
		データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	契約／運用
		権利関連	（5）分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、所有権、活用内容、その可否について合意し契約として締結しておくこと。 補足 7.1 を参照。。	契約／運用
エンドユーザ		データの扱い	（4）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	契約／運用
			（6）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要なるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	運用
		システム設計	（7）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検討すること。	契約／運用
			（8）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	契約／運用
		データの扱い	（9）エンドユーザ NM 内の利用者（エンドユーザ内の従業員）への告知。	従業員からの同意取得について、新たなデータ流通取引に関する検討事例集 ver2.0<検討事例 1-05>を参考。	運用

	ケース 4-2	課題分類	課題／心配事	対応策	対応分類
			（10）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	契約／運用
		システム設計	（11）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（7）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	契約／運用
			（12）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	契約
説明	統計データ（加工データ）のみを上げ、パケットデータの蓄積・提供は無し。				

6.6 ケース 5 端末の位置情報サービス

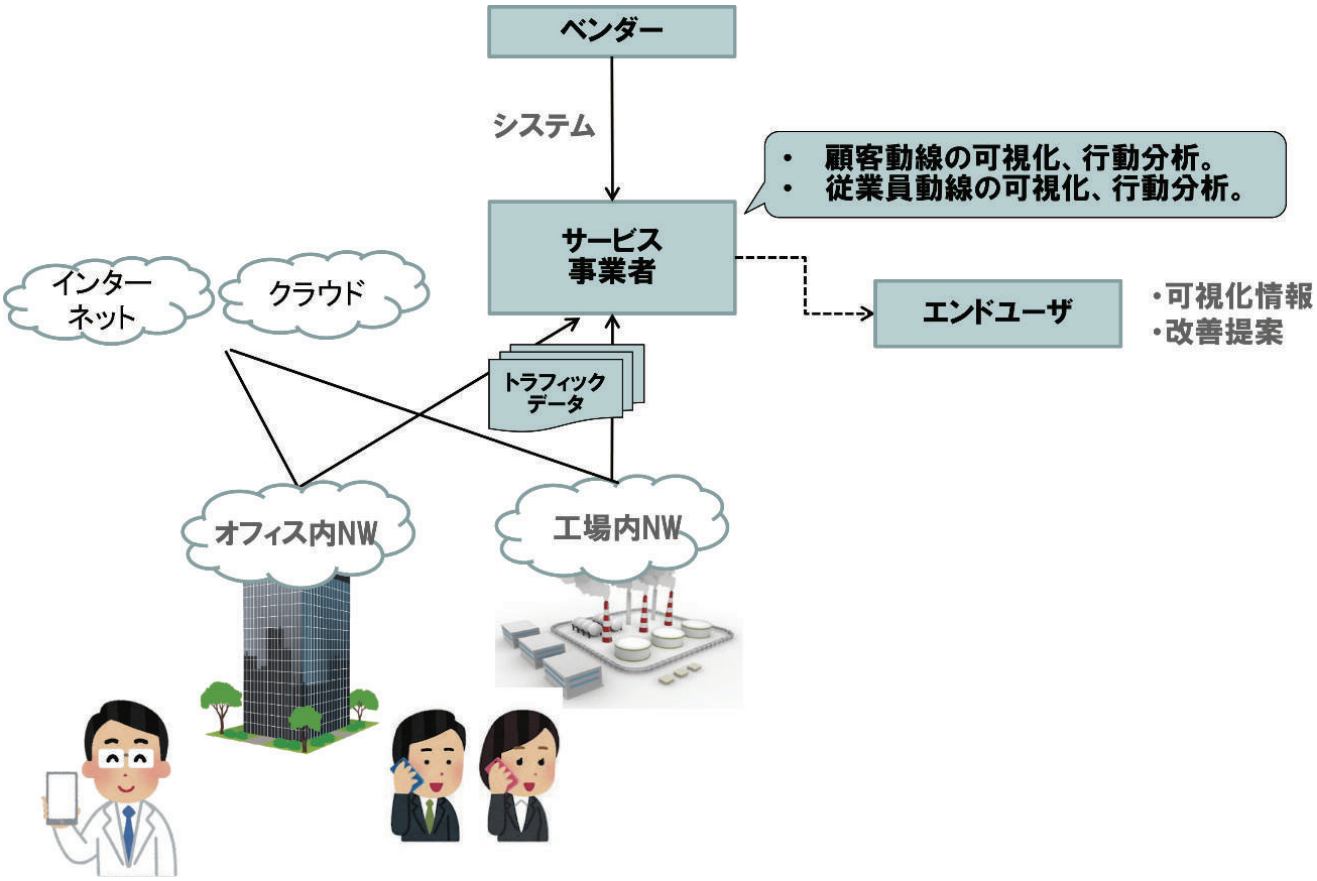
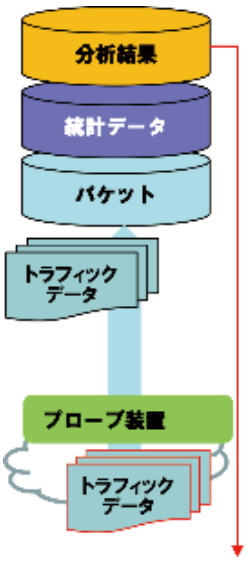


図 6-9

6.6.1 ケース 5-1-1

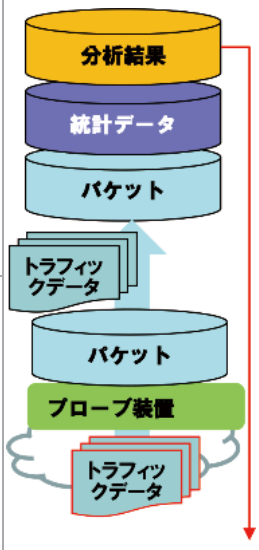
表 6-11

	ケース 5-1-1	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いをどうすればいいのか？	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	契約／運用
				解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	
				消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	
			（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	契約／運用
				上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	
サービス事業者		データの扱い	（1）パケットの PDU 部分にエンドユーザの機密情報などが含まれる可能性があるが、漏洩防止など、どこまでやれば良いのかがわからない。	受領するパケットデータについて、利用目的（行動分析）、利用者（サービス事業者＋エンドユーザ）、取扱いなどを規定した NDA 条項を契約する。	契約／運用
			（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	運用
		システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	運用
		データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	契約／運用
		権利関連	（5）分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、所有権、活用内容、その可否について合意し契約として締結しておくこと。	契約／運用
エンドユーザ		データの扱い	（1）プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。	プローブ内の保管データ／保管期間、送信データなどがサービス仕様内に規定しているか確認し、その内容を確認すること。	運用
			（2）トラフィックデータの PDU に含まれる企業機密・個人情報は ①データとして取り出されるのだろうか？ ②サービス事業者で適切にアクセス管理されるのだろうか？	契約で規定。（上記サービス事業者（1）を参照）	契約／運用
			（3）個人情報を意図せずサービス事業者に渡していないだろうか？	事業者が提示するサービス仕様から、送信されるパケットデータ種別を確認する。パケットデータから個人情報を復元できる場合は、個人情報を渡しているとみなされ得るので、適切な扱いが必要。（詳細は個人情報保護法を参照） 日本では MAC アドレス単体では個人識別性を有しないが、他の情報と容易に照合できる場合は個人識別性をもつ。MAC アドレスとユーザを結び付ける情報を提示有無を確認すること。	法令

	ケース 5-1-1	課題分類	課題／心配事	対応策	対応分類
			（4）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	契約／運用
			（5）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要なるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	運用
			（6） 社内関係者以外（来客 etc）のデータを意図せず収集していないか。	来客用の無線アクセスポイント等は位置情報分析システムの設計から分離しておく、または来客に事前に周知しておく。	運用
		システム設計	（7）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検討すること。	契約／運用
			（8）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	契約／運用
		データの扱い	（9）エンドユーザ NM 内の利用者（エンドユーザ内の従業員）への告知。	従業員からの同意取得について、新たなデータ流通取引に関する検討事例集 ver2.0<検討事例 1-05>を参考。	運用
			（10）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	契約／運用
		システム設計	（11）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（9）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	契約／運用
			（12）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	契約
説明	トラフィックデータをそのまま上げて分析。パケット提供有／無の両ケースあり。				

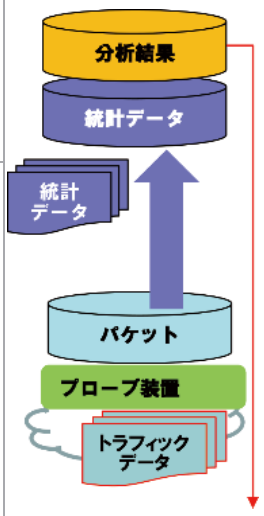
6.6.2 ケース 5-1-2

表 6-12

	ケース 5-1-2	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム障害	【ケース 5-1-1 に追加】 （1）故障発生時にパケット格納装置が返送された際、格納されたデータの取扱いをどうすればいいのか？	ケース 5-1-1 と同じく、返却前にパケット格納装置内のデータを全消去して送付する旨を、マニュアル等記載し、事前に周知しておく。	契約／運用
		システム設計	【ケース 5-1-1 に追加】 プローブ装置に不正にログインされた場合、パケット格納装置内データが盗みとられないか？	多段認証など、不正ログインへの対策と合わせて、パケット格納装置内データへのアクセスセキュリテイを、装置ログインとは別に設けるなど、検討する。	運用のみ
サービス事業者			他は 5-1-1 ケースに従う。上記 2 項を追加。		
エンドユーザ					
説明	パケットデータを上げるが、プローブ装置にも提供用に保存。				

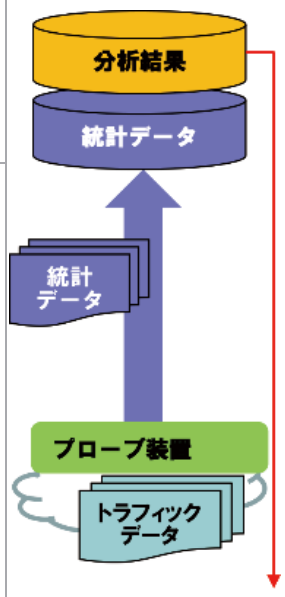
6.6.3 ケース 5-2-1

表 6-13

	ケース 5-2-1	課題分類	課題／心配事	対応策	対応分類
ベンダー		システム障害	【ケース 5-1-1 に追加】 （1）故障発生時にパケット格納装置が返送された際、格納されたデータの取扱いをどうすればいいのか？	ケース 5-1-1 と同じく、返却前にパケット格納装置内のデータを全消去して送付する旨を、マニュアル等記載し、事前に周知しておく。	契約／運用
		システム設計	【ケース 5-1-1 に追加】 プローブ装置に不正にログインされた場合、パケット格納装置内データが盗みとられないか？	多段認証など、不正ログインへの対策と合わせて、パケット格納装置内データへのアクセスセキュリテイを、装置ログインとは別に設けるなど、検討する。	運用のみ
サービス事業者			他は 5-1-1 ケースに従う。		
			（2）トラフィックデータの PDU に含まれる企業機密・個人情報は ①データとして取り出されるのだろうか？ ②サービス事業者で適切にアクセス管理されるのだろうか？ ⇨　送信対象が統計データであるため、対象外。		契約／運用
			（3）個人情報を意図せずサービス事業者に渡していないだろうか？ ⇨　送信対象が統計データであるため、対象外。		法令
			（9）サービス事業者に送られる分析結果には個人を特定できるような情報が含まれていないか？ ⇨　送信対象が統計データであるため、対象外。		法令
説明	統計データのみを上げ、プローブ装置には提供用にパケットデータを保持。				

6.6.4 ケース 5-2-2

表 6-14

	ケース 5-2-2	課題分類	課題／心配事	対応策	対応分類
ベンダー					
サービス事業者			他は 5-1-1 ケースに従う。		
エンドユーザ			(1) プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。 ⇨ 送信対象が統計データであるため、対象外。		
			(2) トラフィックデータの PDU に含まれる企業機密・個人情報は ①データとして取り出されるのだろうか？ ②サービス事業者で適切にアクセス管理されるのだろうか？ ⇨ 送信対象が統計データであるため、対象外。		
			(3) 個人情報を意図せずサービス事業者に渡していないだろうか？ ⇨ 送信対象が統計データであるため、対象外。		
			(9) サービス事業者に送られる分析結果には個人を特定できるような情報が含まれていないか？ ⇨ 送信対象が統計データであるため、対象外。		
説明	統計データのみを上げ、パケットデータ提供は無し。				

6.7 項目とユースケースの対応表

表 6-15

	課題分類	課題／心配事	対応策	番号	ケース 1-1-1	ケース 1-1-2	ケース 1-2-1	ケース 1-2-2	ケース 2	ケース 3	ケース 4	ケース 5
ベンダー	システム設計	（1）故障発生時にプローブ装置などが返送された際、設定やログにエンドユーザに固有の情報（IP アドレスなど）が含まれるが、それらの取扱いをどうすればいいのか？	返品は初期化されることを予め通知しておく。その上で、必要なデータを抽出後、確実に初期化を実施。抽出したデータは解析目的のみの利用とする。	1	○	○	○	○				
			解析に必要な障害ログ、内部情報はファイル化し、セキュアなファイル転送サービスで受信する方法を事前に確立しておく。輸送時に機器に残さない。 契約書、マニュアルに記載すること。	2	○	○	○	○				
			消去無しで機器を輸送する際には、運送会社のセキュア便などの利用を検討することが望ましい。	3	○	○	○	○				
		（2）ユーザから転送された、ログ情報等の扱いについて。	転送されたデータは解析目的のみの利用とすることを契約書、マニュアルに記載。解析後のデータ廃棄についても取り決め、明記しておくことが望ましい。	4	○	○	○	○				
			上記方法がとれない場合、データの扱いについて契約書にて規定し合意しておく。	5	○	○	○	○				
		（3）プローブ装置に不正にログインされた場合、パケット格納装置内データが盗みとられないか？	多段認証など、不正ログインへの対策と合わせて、パケット格納装置内データへのアクセスセキュリテイを、装置ログインとは別に設けるなど、検討する。	6	-	○	○	-				
	システム障害	（4）故障発生時にパケット格納装置が返送された際、格納されたデータの取扱いをどうすればいいのか？	ケース 1-1-1 と同じく、返却前にパケット格納装置内のデータを全消去して送付する旨を、マニュアル等記載し、事前に周知しておく。	7	-	○	○	-				
セキュリティサービス事業者	データの扱い	（1）パケットの PDU 部分にエンドユーザの機密情報などが含まれる可能性があるが、漏洩防止など、どこまでやれば良いのかがわからない。	受領するパケットデータについて、利用目的（セキュリティ分析）、利用者（サービス事業者＋エンドユーザ）、取扱いなどを規定した NDA 条項を契約する。	8	○	○	○	○				
		（2）分析結果はトラフィックデータに基づいて自社が生成した情報だが、エンドユーザを特定するような部分を匿名化するなどした上で、他のエンドユーザ向けの分析に活用するといったことはできないのか？	（1）に記載の契約内容に反しない内容であれば利用可能。	9	○	○	○	○				
	システム設計	（3）データ送信の通信路の安全性について。	通信路はセキュアである必要があるかを合意しておく。専用線でなければ、VPN 等のセキュア通信路を確立しておくこと。	10	○	○	○	○				

	データの扱い	（4）パケットデータ、統計データの機密扱いについて。 ・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。	サービス仕様として明文化しておくこと。契約書にて規定し、双方合意を得ること。	11	○	○	○	○				
	権利関連	（5）分析結果から派生するデータ（例えば、振る舞い検知などのパターンデータ）について、所有者、活用について、事前に合意しておくこと。	契約事項として、所有権、活用内容、その可否について合意し契約として締結しておくこと。 補足 7.1 を参照。。	12	○	○	○	○				
エンドユーザ	データの扱い	（1）プローブ装置にどんなデータが溜め込まれるのか？サービス事業者にどんなデータが送られるのか？がわからないので心配。	プローブ内の保管データ／保管期間、送信データなどがサービス仕様内に規定しているか確認し、その内容を確認すること。	13	○	○	○	-				
		（2）トラフィックデータの PDU に含まれる企業機密・個人情報は ①データとして取り出されるのだろうか？ ②サービス事業者で適切にアクセス管理されるのだろうか？	契約で規定。（上記サービス事業者（1）を参照）	14	○	○	-	-				
		（3）個人情報を意図せずサービス事業者に渡していないだろうか？	事業者が提示するサービス仕様から、送信されるパケットデータ種別を確認する。パケットデータから個人情報を復元できる場合は、個人情報を渡しているとみなされ得るので、適切な扱いが必要。（詳細は個人情報保護法を参照） 日本では MAC アドレス単体では個人識別性を有しないが、他の情報と容易に照合できる場合は個人識別性をもつ。MAC アドレスとユーザを結び付ける情報を提示有無を確認すること。	15	○	○	-	-				
		（4）サービス事業者が当社のデータを他社に提供していないことをどうやったら確認できるのだろうか？	NDA 条項等により第 3 者への提供を制限することは可能だが、確認手段は提供されない。必要に応じて契約内で規定する必要あり。	16	○	○	○	○				
		（5）異常を検知した際に、該当するパケットデータも送られてくるのはいいが、その PDU に含まれる企業機密／個人情報の管理が難しい（オリジナルの情報であれば社内のルールに従って管理される）	（ポイント）まずはデータが返送されるサービスの有無の確認。ある場合、自社データではあるが、管理部署とは違う部署にデータが送られる場合、管理上問題になるか否か事前に確認しておくこと。 別途、受領パケットデータの取扱いについて規定が必要。	17	○	○	○	○				
		（6）サービス事業者の拠点が海外にありデータが越境する場合、輸出管理が必要なるか否か。	自社の輸出管理部門に相談。必要な手続きを実施する。	18	○	○	○	○				

	システム設計	（7）プローブ装置に対して、サービス事業者／ベンダーがリモート制御を行う際、セキュリティが心配。	装置へのアクセスは、ユーザ認証の他にワンタイムパスワードなどで多段認証とすることを推奨する。また、事業者の悪意ある操作に対しては、損害賠償条項を織り込むなどを検討すること。	19	○	○	○	○				
		（8）プローブ装置が故障した際、自社 NW がダウンしないか？また、万一、プローブ装置が原因で自社 NW の正常な運用が妨げられた場合に、損害を補償してくれるのか？	装置故障時の自社 NW への影響を、サービス事業者に確認し明確化しておく。必要に応じて、TAP 装置など影響を最小化する施策を講じることが望ましい。 自社 NW への影響がある場合、有事の際の、責任の所在、その対応について事前に合意しておくこと。さらに、契約として損害賠償規定が定められているかどうかを確認。外部の保険を利用する選択肢もあり。	20	○	○	○	○				
	データの扱い	（9）エンドユーザ NM 内の利用者（エンドユーザ内の従業員）への告知。	従業員からの同意取得について、新たなデータ流通取引に関する検討事例集 ver2.0<検討事例 1-05>を参考。	21	○	○	-	-				
		（10）分析結果の保存ポリシーはどうなっているのか。過去の分析結果を削除する際の方法など。完全に削除されるのか。	・保管データ種別、保管方法、保管期間の明確化。 ・保管データの廃棄方法、確認方法の明確化。 事業者からのサービス仕様を確認すること。	22	○	○	○	○				
	システム設計	（11）保守の際やシステムのアップデートの際にプローブ装置および関連システム以外にアクセスされないようになっているか。	上記エンドユーザ（7）に加え、事業者が設置した装置（関連を含む）以外へのアクセス／影響を、事業者に確認する。 それ以外へのアクセス禁止を契約に合意しておくことが望ましい。	23	○	○	○	○				
		（12）プローブ装置自体の脆弱性有無についての情報がサービス事業者からタイムリーに得られるのか？	問合せへの回答や、定期レポートなどで脆弱性有無に関する情報や、脆弱性がある場合の対処策についての情報が得られることを契約で確認しておく。	24	○	○	○	○				

7. 補足

7.1 契約における留意事項

（1）サービス事業者

（1-1）契約記載の必要性と参考ガイドライン

サービス事業者が、サービス利用者に対してトラフィックデータ収集により各種分析サービスを提供する場合、データや学習済モデル等に関わる権利について契約に記載しておくことが推奨される。特に、データは民法上の所有権の対象でないため、契約上記載がない場合、その利用権限は、曖昧な状態になってしまうことがあり留意が必要である。

データや AI に関しての契約の基本的考え方や検討プロセス等については、下記ガイドラインが参考となる。

－データの利用権限に関する契約ガイドライン（2017 年 5 月 IoT 推進コンソーシアム、経済産業省）

－AI・データの利用に関する契約ガイドライン（2018 年 6 月 経済産業省）

（1-2）関連ガイドラインの参照ポイント

前記の二つの関連ガイドラインにおいて、トラフィックデータ収集関連サービスに関して、特に参考となると思われる点を記しておく。

（1-2-1）データの利用権限に関する契約ガイドライン（2017 年 5 月）

掲記ガイドライン内の「ケース別の適用例　事例 2」が本ガイドラインの想定ケースに近い。事例 2 においては、データをインプットデータ、学習済モデル等のアルゴリズム、アウトプットデータの三つへ分類し、アルゴリズム及びアウトプットデータに関して利用権限の契約への記載内容について検討が行われている。アルゴリズムやアウトプットデータに関しての検討内容は、トラフィックデータ収集関連サービスの契約検討においても有効と思われる。一方、インプットデータに関しては、取引において新たに発生したデータではないことから、事例 2 では検討の対象外となっている。

（1-2-2）AI・データの利用に関する契約ガイドライン（データ編・AI 編）（2018 年 6 月）

掲記ガイドラインは、データ編と AI 編の大きく二つに分かれており、主にデータ自体に関する契約事項はデータ編に、学習済モデル等のプログラムを含む契約事項は AI 編に書かれている。

データ編においては、契約上のモデル分類としてデータ提供型、データ創出型、データ共有型（プラットフォーム型）の三つに分類している。本ガイドラインの対象としては、データ提供型、及びデータ創出型の検討内容が参考となる。データ共有型（プラットフォーム型）は、多数のデータ提供・利用者間でのデータ相互活用を目的としたもので、相対契約ではなく利用規約での管理を目指す内容となっている。

データ提供型における検討は、トラフィックデータ収集のインプットデータ（生データ）の扱いを検討する上での参考となる。またデータ創出型における検討は、（d11）の事例とも重複するが、インプットデータ及びアウトプットデータの扱いについて検討する上での参考となる。双方において、データの利用目的の限定が求められているが、トラフィックデータ収集のユースケースにおいても、

インプットデータ及びアウトプットデータを区別した上で、利用目的を限定することが有効であろう。

AI 編においては、機械学習により価値創出がなされるモデルにおいての契約上の考慮事項が記載されている。検討対象として、生データ、学習用データセット、学習用プログラム、学習済モデル（学習済パラメータ、推論プログラム）等が上げられており、想定される前提条件毎に契約の記載案が上げられている。プログラムは知的財産権（著作権、特許権等）によって保護されるが、生データ、派生データは基本的には知的財産権の対象外となるため、利用条件の規定によって、その利用権限や制限を定めていく、ということが一つのポイントであろう。また、データに個人情報が含まれる場合の契約上の対応案についても、条項として取り上げられている。

（1-3）トラフィックデータ収集サービスにおける検討ポイント

該当サービスが、サービス利用者のデータを活用して機械学習、ディープラーニング等の AI により学習モデルを創出していく場合、前記関連ガイドラインの AI に関わる部分の内容が参考となる。AI を用いない場合は、分析プログラムの知的財産権は基本的にはサービス事業者に帰属するため、関連データの利用条件について、関連ガイドラインのデータに関わる部分を参考としていくことになる。

AI を用いる／用いないに関わらず、トラフィックデータ収集サービスにおいては、ネットワーク上を流れるトラフィックデータを各種分析のために収集するため、インプットデータ（生データ）の利用条件に関しては、利用目的等含め、記載を行っておくことが望ましい。

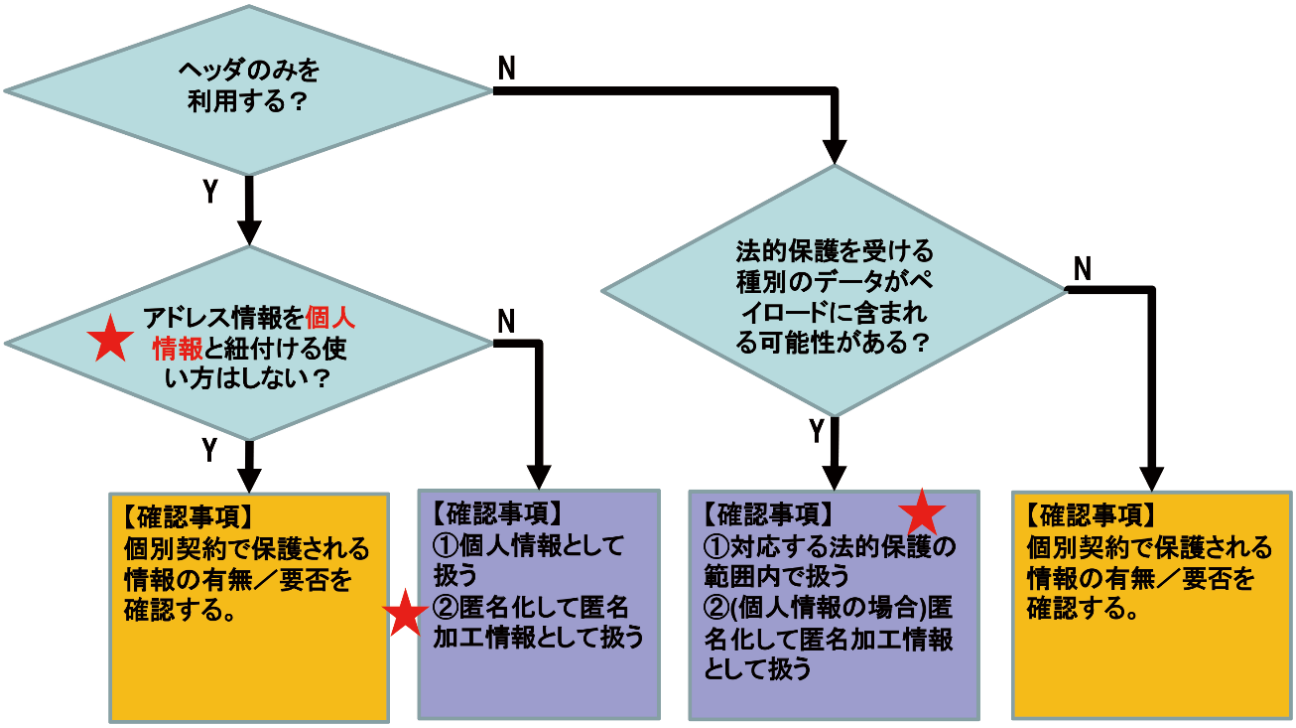
インプットデータ（生データ）のペイロード部に個人情報等が含まれる場合には、その取り扱いに関して考慮が必要となる。ペイロード部は暗号化されている場合も多いと思われるが、システム利用者からシステム事業者へ提供されるデータ内に、システム事業者が識別可能な個人情報が含まれることを想定する場合には、前記関連ガイドラインの個人情報の条項が参考となる。

また、直接の個人情報ではないが、ヘッダ部に含まれる MAC アドレス（*1）や IP アドレスのようなアドレス情報についても、その扱いについて考慮しておく必要がある。MAC アドレスや IP アドレスは、一般的にインプットデータ（生データ）には含まれことが多いと思われる。そのためインプットデータ（生データ）の利用目的の明確化、及びアウトプットデータにおけるアドレス情報の必要に応じた匿名化などの利用条件の規定を行うことが想定される。

*1 MAC アドレスと個人情報との紐付きに関して、「新たなデータ流通取引に関する検討事例集」（2018 年 8 月 IoT 推進コンソーシアム、総務省、経済産業省）内で、国内ではそれ自体で個人情報にはあたらないが、他情報との紐付けされた場合、個人識別性を有する可能性もあるとされている。

7.2 パケットデータの取扱い

● データ漏洩　⇔　データ取得　のリスクは？



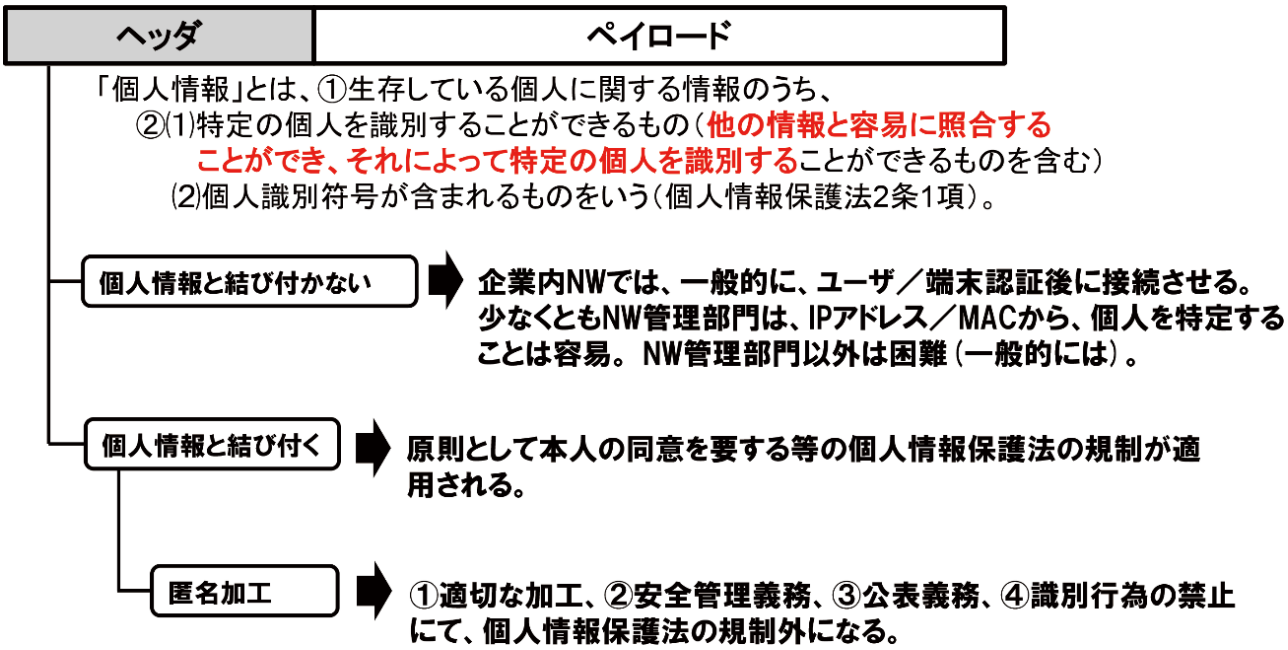


図 7-1

ヘッダ	ペイロード

データ種別に応じて法的保護の対象となるが、必ずしも保護対象になるのかグレーゾーンは存在する。契約などの手段をガイドする。

データ種別		該当法律	保護要件
著作物		著作権法	創作性の有無。機械的に創出されるデータに創作性が認められる場合は限定的。
営業秘密		不正競争防止法	①非公知性、②事業的有用性、**③秘密管理性**の 3 つの要件を充たすもの。
限定提供データ		不正競争防止法	①限定提供性、②電磁的管理性、**③相当蓄積性**の3つの要件を充たすもの。
パーソナルデータ	個人情報	個人情報保護法	①生存する個人の情報、②特定の個人を識別することができる情報。
	匿名加工情報		①適切な加工、②安全管理義務、③公表義務、④識別行為の禁止、の4つの順守義務あり。

秘密管理性：その情報に合法的かつ現実に接触することができる従業員等からみて、その情報が会社にとって秘密としたい情報であることが分かる程度に、**アクセス制限**やマル秘表示といった秘密管理措置がなされていること。外部クラウドを利用して営業秘密を保管・管理する場合も、秘密として管理されていれば秘密管理性が失われるわけではない。
→ アクセス制限がある場所にある営業秘密は、NW上においても保護対象である。

図 7-2

おわりに

トラフィックデータ活用にて様々な価値が生み出され、生活がより豊かになると期待する。

本ガイドラインをご活用頂き、その一助となれば幸いである。