資料3-2

# TTCにおける検討状況
# 【非機能要件】

# システムに求める各種要求水準（非機能要件）（１／７）

## ●検討方針

Net１１９通報システムの信頼性等の確保に必要な項目、内容、水準はどのようなものか検討する。

検討にあたっては、Net１１９に求められる共通的かつ最低限必要となる要求水準の検討が必要となるため、共通電文の検討と同様に、一般社団法人情報通信技術委員会（TTC）に検討を依頼する。

## ●検討手順

Net１１９導入にあたり、最低限満たすべき非機能要求のレベルを定義するにあたり、メトリクス（指標）の抽出、レベル設定について、以下の手順で進める。

・独立行政法人情報処理推進機構（IPA）で公開している「非機能要求グレード」から必要となるメトリクスを抽出
（システム特性（利用者・業務・方式）、共通定義可能な項目かどうか等の観点で抽出）
↓
・各メトリクスのレベルを設定
（既存・類似システムのレベル、法律・条令、コスト等を考慮して設定）

# システムに求める各種要求水準（非機能要件）（2／7）

## ●検討結果

Net119通報システムの非機能要件の内容、レベルについて、一般社団法人情報通信技術委員会（TTC）にて検討した結果は以下の表の通り。

| 項番 | 大項目 | 中項目 | 小項目 | メトリクス（指標） | 設定レベル | 設定理由、条件等 |
|---|---|---|---|---|---|---|
| A.1.1.1 | 可用性 | 継続性 | 運用スケジュール | 運用時間（通常） | 24時間無停止 | 119番通報という特性から無停止での運用が必要である。 |
| A.1.1.2 | | | | 運用時間（特定日） | 24時間無停止 | 119番通報という特性から無停止での運用が必要である。 |
| A.1.1.3 | | | | 計画停止の有無 | 計画停止無し | 119番通報という特性から無停止での運用が必要である。 |
| A.1.2.1 | | | 業務継続性 | 対象業務範囲 | 全ての業務 | 事業者間連携における処理を含む通報、通報受理に必要な全ての業務とする。（ただし、通報に関係しない管理系機能などは除く） |
| A.1.3.1 | | | 目標復旧水準（業務停止時） | RPO（目標復旧地点） | 障害発生時点（日次バックアップ+アーカイブからの復旧） | 通報内容など、データの損失は許容できないため、障害発生時点までの復旧する必要がある。 |
| A.1.3.3 | | | | RLO（目標復旧レベル） | 事業者間連携における処理を含む通報、通報受理に必要な全ての業務 | 通報に関係しない管理系機能などは除く |
| A.1.4.1 | | | 目標復旧水準（大規模災害時） | システム再開目標 | 再開不要 | DRサイトへ切り替え、そちらでの運用になるため再開目標は規定しない。 |
| A.1.5.1 | | | 稼働率 | 稼働率 | 99.999% | 重要な社会インフラである金融システムでも「99.999%」（障害による年間合計停止時間5分以内）であり、稼働率目標は、「「99.999%」が高い目標という社会通念がある。<br>また、稼働率の条件は以下の通り<br>・対象範囲はNet119GWとする。<br>・事業者間連携の連携先の停止は含まず。<br>・外部要因（例：DDoS攻撃などによるサービス停止等）を除く。 |

出典：一般社団法人情報通信技術委員会（TTC） 緊急通報アクセシビリティSWG第4回会合資料

# システムに求める各種要求水準（非機能要件）（3／7）

| 項番 | 大項目 | 中項目 | 小項目 | メトリクス（指標） | 設定レベル | 設定理由、条件等 |
|---|---|---|---|---|---|---|
| A.2.1.1 | | 耐障害性 | サーバ | 冗長化（機器） | 全てのサーバで冗長化 | 24時間無停止の要求レベル達成のため、冗長化が必要である。 |
| A.2.2.1 | | | 端末 | 冗長化（機器） | 業務や用途毎に予備端末を設置 | 消防の通報受理端末を対象とする。 |
| A.2.3.1 | | | ネットワーク機器 | 冗長化（機器） | 全ての機器を冗長化 | 24時間無停止の要求レベル達成のため、冗長化が必要である。 |
| A.2.4.1 | | | ネットワーク | 回線の冗長化 | 全て冗長化する | 24時間無停止の要求レベル達成のため、冗長化が必要である。 |
| A.2.4.2 | | | | 経路の冗長化 | 全て冗長化する | 24時間無停止の要求レベル達成のため、冗長化が必要である。 |
| A.2.5.1 | | | ストレージ | 冗長化（機器） | 全て冗長化する | 24時間無停止の要求レベル達成のため、冗長化が必要である。 |
| A.2.6.1 | | | データ | バックアップ方式 | オンラインバックアップ | 無停止が前提となることから、稼働中の状態でバックアップを取得することが必要である。 |
| A.2.6.2 | | | | データ復旧範囲 | システム内の全データを復旧 | 119番通報という特性、および事後のトレース等を考慮すると、全データを復旧しておく必要がある。 |
| A.3.1.1 | | 災害対策 | システム | 復旧方針 | 同一の構成をDRサイトで構築 | 災害時でも119番通報を受理できる必要がある。 |
| A.3.2.1 | | | 外部保管データ | 保管場所分散度 | 1ヵ所(300km以上離れた遠隔地) | 遠隔地のDRサイトへ保管する。 |
| A.3.2.2 | | | | 保管方法 | DRサイトへのリモートバックアップ | 遠隔地のDRサイトへのバックアップとなるため、リモートで行う必要がある。 |
| A.3.3.1 | | | 付帯設備 | 災害対策範囲 | 想定する全ての対策を実施する | 災害時でも119番通報を受理できる状態にしておく必要があることから、想定する全ての対策を講じる。（データセンター要件） |

出典：一般社団法人情報通信技術委員会（TTC） 緊急通報アクセシビリティSWG第4回会合資料

# システムに求める各種要求水準（非機能要件）（4／7）

| 項番 | 大項目 | 中項目 | 小項目 | メトリクス（指標） | 設定レベル | 設定理由、条件等 |
|---|---|---|---|---|---|---|
| B.1.1.1 | 性能・拡張性 | 業務処理量 | 通常時の業務量 | ユーザ数 | 上限が決まっている | 利用登録者は管轄内の聴覚障がい者、また、事業者間転送でアクセスしてくる利用者の最大上限は全国の聴覚障がい者となるが、導入消防にて想定利用者数を定義する必要がある。（訪日外国人の利用は現時点で考慮しない） |
| B.1.1.2 | | | | 同時アクセス数 | 同時アクセスの上限が決まっている | 消防で受理できる端末数とする。 |
| B.1.3.1 | | | 保管期間 | 保管期間 | 1年 | 通報のアクセスをトレースするなどが想定されるため、最低1年は保管する必要がある。 |
| B.1.3.2 | | | | 対象範囲 | アーカイブまで含める | アクセス、通信ログ、通報履歴データ等を対象範囲とする。 |
| B.2.1.1 | | 性能目標値 | オンラインレスポンス | 通常時レスポンス順守率 | 99%以上 | チャット機能におけるレスポンス1秒を順守する。<br>ただし、外部要因（例：インターネット経路における遅延等）を除く。 |
| B.2.3.2 | | | オンラインスループット | ピーク時処理余裕率 | 同時アクセス数の10倍以上 | 10倍以上の状況において、利用できる必要がある。 |
| C.1.1.1 | 運用・保守性 | 通常運用 | 運用時間 | 運用時間（通常） | 24時間無停止 | 119番通報という特性から無停止での運用が必要である。 |
| C.1.1.2 | | | | 運用時間（特定日） | 24時間無停止 | 119番通報という特性から無停止での運用が必要である。 |
| C.1.2.1 | | | バックアップ | データ復旧範囲 | システム内の全データを復旧 | 119番通報という特性、および事後のトレース等を考慮すると、全データを復旧しておく必要がある。 |
| C.1.2.5 | | | | バックアップ取得間隔 | 同期バックアップ | 災害時にDRサイトへ切り替えし、すぐに運用可能とする必要があるため、同期バックアップが必要である。 |
| C.1.2.6 | | | | バックアップ保存期間 | 1年 | 通報のアクセスをトレースするなどが想定されるため、最低1年は保管する必要がある。 |
| C.1.3.1 | | | 運用監視 | 監視情報 | リソース監視を行う | 24時間無停止、安定稼働のため、パフォーマンス監視を行う必要がある。 |
| C.1.3.2 | | | | 監視間隔 | リアルタイム監視（秒間隔） | 障害発生時を迅速に検知する必要があることから、秒間隔での監視を行う必要がある。ただし、監視情報収集がパフォーマンスに影響を与えない程度の間隔とする。 |
| C.1.4.1 | | | 時刻同期 | 時刻同期設定の範囲 | システム全体を外部の標準時間と同期する | 通報受理等において、正確な時刻が求められるため、標準時間との同期が必要である。 |

出典：一般社団法人情報通信技術委員会（TTC） 緊急通報アクセシビリティSWG第4回会合資料

# システムに求める各種要求水準（非機能要件）（5／7）

| 項番 | 大項目 | 中項目 | 小項目 | メトリクス（指標） | 設定レベル | 設定理由、条件等 |
|---|---|---|---|---|---|---|
| C.2.1.1 | | 保守運用 | 計画停止 | 計画停止の有無 | 計画停止無し | 119番通報という特性からシステムを停止できる時間帯が存在しない。 |
| C.4.2.1 | | | 試験用環境の設置 | 試験用環境の設置有無 | 専用の試験用環境を設置する | 事業者関連携の試験実施の際、本番環境での接続以前に試験環境との試験が必要があるため、専用の環境を準備しておく必要がある。 |
| C.4.5.1 | | | 外部システム接続 | 外部システムとの接続有無 | 外部システムと接続する | 事業者関連連携に関わる詳細は共通電文仕様書に基づくものとする。 |
| E.1.1.1 | セキュリティ | 前提条件・制約条件 | 情報セキュリティに関するコンプライアンス | 順守すべき社内規程、ルール、法令、ガイドライン等の有無 | 有り | ◆順守すべき法令、条令等<br>・個人情報保護法<br>・地方公共団体における情報セキュリティポリシーに関するガイドライン<br>・電気通信事業における個人情報保護に関するガイドライン<br>◆事業者としての資格<br>・ISO 27001<br>・プライバシーマーク |
| E.3.1.1 | | セキュリティ診断 | セキュリティ診断 | ネットワーク診断実施の有無 | 有り | 利用者情報等の漏えいリスク低減のため、定期的なセキュリティ監査が必要である。<br>ただし、実施頻度、範囲は協議のうえ決定する。 |
| E.3.1.2 | | | | Web診断実施の有無 | 有り | 利用者情報等の漏えいリスク低減のため、定期的なセキュリティ監査が必要である。<br>ただし、実施頻度、範囲は協議のうえ決定する。 |
| E.4.3.1 | | | セキュリティパッチ適用 | セキュリティパッチ適用範囲 | システム全体 | 部分的ではく、システム全体を適用範囲とする。 |
| E.4.3.2 | | | | セキュリティパッチ適用方針 | 緊急性の高いセキュリティパッチのみ適用 | パッチ適用による影響確認の作業負担を考慮し、緊急性の高いセキュリティパッチのみ適用とする。<br>また、システム全体への影響を確認し、パッチ適用の可否を判断する |
| E.4.3.3 | | | | セキュリティパッチ適用タイミング | パッチ出荷時に実施 | 緊急性の高いパッチについては、影響確認後、速やかに適用する必要がある。 |

出典：一般社団法人情報通信技術委員会（TTC） 緊急通報アクセシビリティSWG第4回会合資料

# システムに求める各種要求水準（非機能要件）（6／7）

| 項番 | 大項目 | 中項目 | 小項目 | メトリクス（指標） | 設定レベル | 設定理由、条件等 |
|---|---|---|---|---|---|---|
| E.6.1.1 | | データの秘匿 | データ暗号化 | 伝送データの暗号化の有無 | 重要情報を暗号化 | 通報内容等は重要情報であるため、暗号化が必要である。 |
| E.6.1.2 | | | | 蓄積データの暗号化の有無 | 重要情報を暗号化 | 利用者情報、通報ログなど重要情報であるため、暗号化が必要である。 |
| E.7.1.1 | | 不正追跡・監視 | 不正監視 | ログの取得 | 実施する | 119番通報という特性から取得しておく必要がある。 |
| E.7.1.2 | | | | ログ保管期間 | 1年 | 通報のアクセスをトレースするなどが想定されるため、最低1年は保管する必要がある。 |
| E.7.1.3 | | | | 不正監視対象（装置） | 重要度が高い資産を扱う範囲、あるいは、外接部分 | 利用者情報など重要情報を扱う部分、公開層について監視する必要がある。監視対象は協議のうえ定義する。 |
| E.7.1.4 | | | | 不正監視対象（ネットワーク） | 重要度が高い資産を扱う範囲、あるいは、外接部分 | 利用者情報など重要情報を扱う部分、公開層について監視する必要がある。監視対象は協議のうえ定義する。 |
| E.7.1.5 | | | | 不正監視対象（侵入者・不正操作等） | システム全体 | 重要システムのため、設置場所のセキュリティが確保される必要がある。 |
| E.8.1.1 | | ネットワーク対策 | ネットワーク制御 | 通信制御 | 有り | 踏み台攻撃等の脅威や、情報の持ち出しを抑止するために、不正な通信を遮断等のネットワーク制御を実施する必要がある。 |
| E.8.2.1 | | | 不正検知 | 不正通信の検知範囲 | システム全体 | 不正な通信を確認し、対策を迅速に実施すうために、不正検知を実施する必要がある。 |
| E.8.3.1 | | | サービス停止攻撃の回避 | ネットワークの輻輳対策 | 有り | 可用性の要求レベル達成のため、サービス停止攻撃への対策を講じる必要がある。 |
| E.9.1.1 | | マルウェア対策 | マルウェア対策 | マルウェア対策実施範囲 | システム全体 | マルウェアの感染により、重要情報が漏洩する脅威等に対抗するために、マルウェア対策を実施する必要がある。 |
| E.10.1.1 | | Web対策 | Web実装対策 | セキュアコーディング、Webサーバの設定等による対策の強化 | 対策の強化 | Webシステムであることから、Webサーバに対する対策を講じる必要がある。 |

出典：一般社団法人情報通信技術委員会（TTC） 緊急通報アクセシビリティSWG第4回会合資料

# システムに求める各種要求水準（非機能要件）（7／7）

| 項番 | 大項目 | 中項目 | 小項目 | メトリクス(指標) | 設定レベル | 設定理由、条件等 |
|---|---|---|---|---|---|---|
| F.1.1.1 | システム環境・エコロジー | システム制約/前提条件 | 構築時の制約条件 | 構築時の制約条件 | 制約有り(全ての制約を適用) | ◆順守すべき法令、条令等<br>・個人情報保護条法<br>・地方公共団体における情報セキュリティポリシーに関するガイドライン<br>・電気通信事業における個人情報保護に関するガイドライン<br>◆事業者としての資格<br>・ISO 27001<br>・プライバシーマーク |
| F.1.2.1 | | | 運用時の制約条件 | 運用時の制約条件 | 制約有り(全ての制約を適用) | ◆順守すべき法令、条令等<br>・個人情報保護条法<br>・地方公共団体における情報セキュリティポリシーに関するガイドライン<br>・電気通信事業における個人情報保護に関するガイドライン<br>◆事業者としての資格<br>・ISO 27001<br>・プライバシーマーク |
| F.2.1.1 | | システム特性 | ユーザ数 | ユーザ数 | 上限が決まっている | 事業者間転送でアクセスしてくるユーザを考慮すると、最大上限は全国の聴覚障がい者の人数と定義する。<br>（訪日外国人の利用は現時点で考慮しない） |
| F.4.1.1 | | 機材設置環境条件 | 耐震/免震 | 耐震震度 | 震度6強相当（500ガル） | 新耐震基準における震度6強相当レベルの耐震性が必要がある。 |
| F.4.4.4 | | | | 停電対策 | 1日間 | 停電時は、DRサイトでの運用になることが想定されるが、最低24時間は自家発電等により、電源供給が図られる必要がある。 |
| 独自追加 | | | | データセンター設置場所 | 国内 | データセンターは国内とする。<br>（情報保管場所を国内に限定している自治体等があるため） |
| 独自追加 | | | | ユーザアカウント有効期間 | 1年 | 使用していないアカウントを削除、メンテナンスする必要がある。アカウントの削除は自治体のルールに基づき消防が実施することとする。 |
| 独自追加 | 運用・保守性 | 通常運用 | 消防側受信設備 | 冗長化 | 2重化 | 通報受理端末・NW回線・ISPを二重化しない場合、通報を于kれない状態になることを避ける。（回線工事等で頻繁に不通になるケースがあるため） |

出典：一般社団法人情報通信技術委員会（TTC） 緊急通報アクセシビリティSWG第4回会合資料