次期行動計画の策定に向けた重要インフラ分野におけるIT環境変化及び実態調査報告書

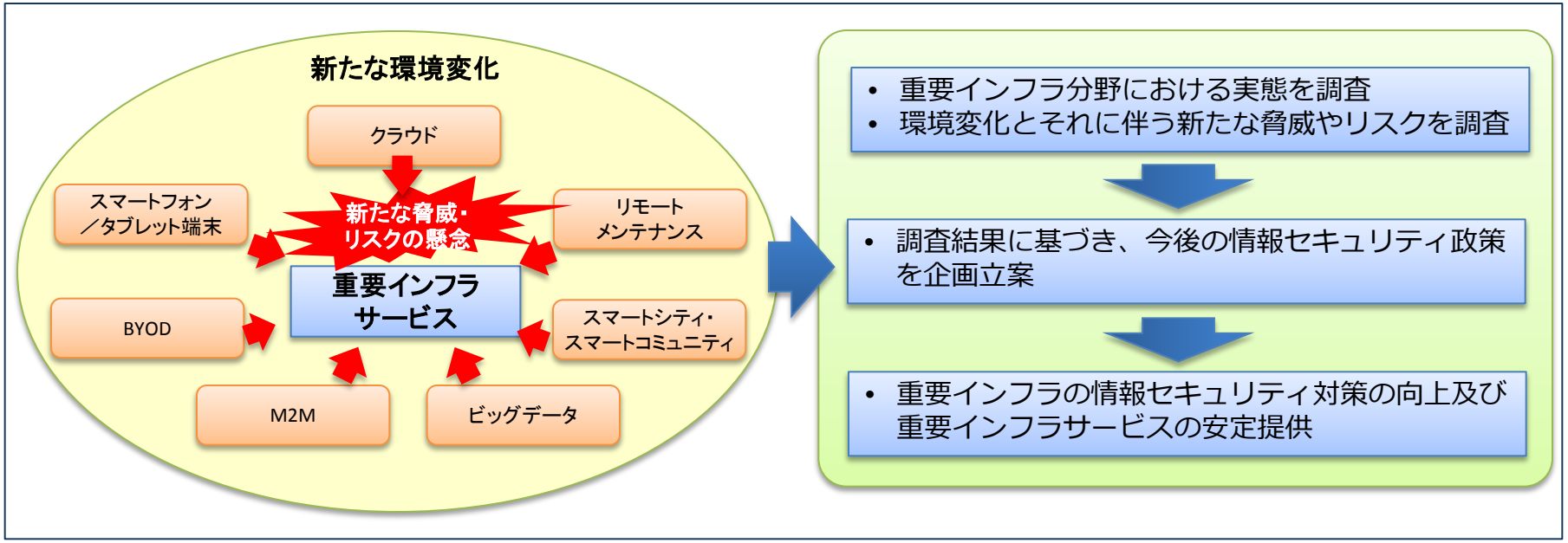
平成２６年３月

株式会社情報通信総合研究所

1. 調査の背景と目的

- 重要インフラの情報セキュリティを取り巻く社会環境や技術環境は刻々と変化している。重要インフラサービスの情報セキュリティ対策の有効性を保ち続けるには、環境変化を的確に捉え、機敏に対応させていく必要がある。
- これを踏まえ、本調査では、重要インフラ分野における情報セキュリティに係る設備・技術等の実態を調査するとともに、将来想定される情報セキュリティに関する環境変化やそれに伴って発生する新たな脅威やリスクについての調査を行う。
- 調査結果については、NISCにおける今後の情報セキュリティ政策の企画立案に活用し、重要インフラの情報セキュリティ対策の向上及び重要インフラサービスの安定提供に資することを目的とする。

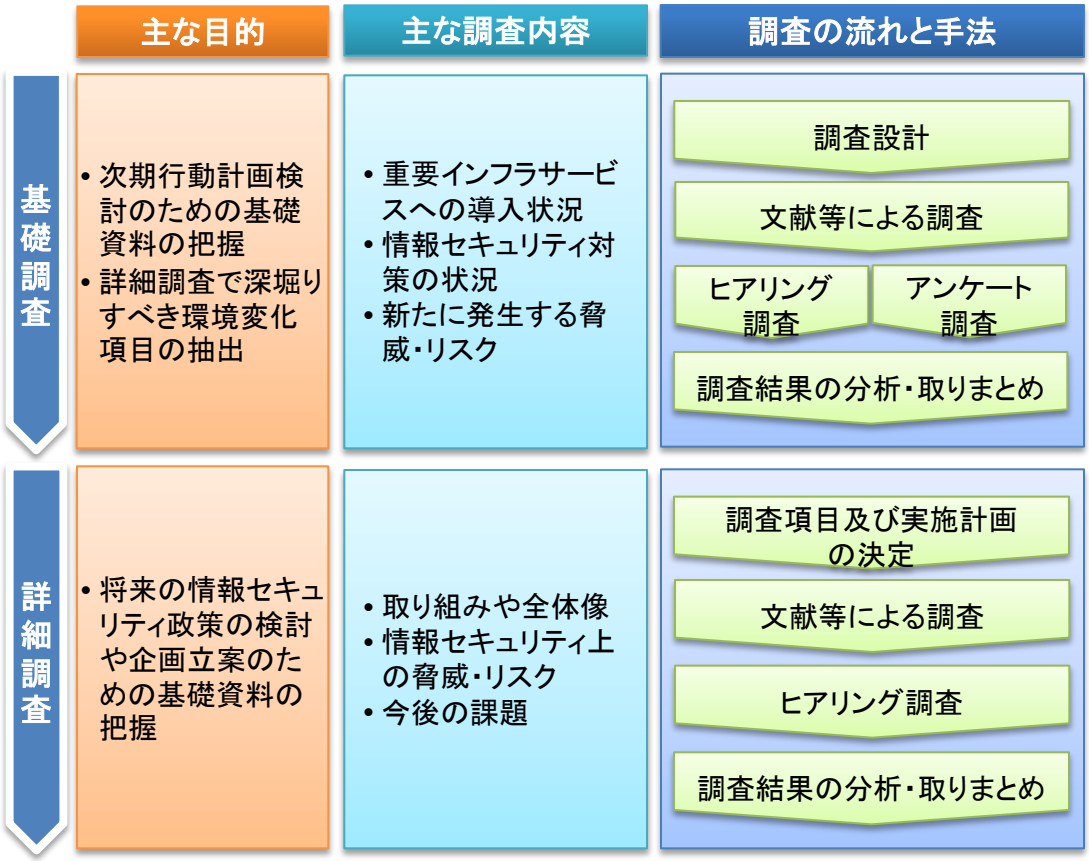
【図表1】調査の背景と目的



2. 調査の全体像

- 調査全体の流れは【図表2】に示すとおり、基礎調査、詳細調査の2段階に分けて進めた。
- 基礎調査では、【図表3】に示す環境変化について、主に次期行動計画の検討のための基礎資料を得るとともに、詳細調査で深堀すべき環境変化の項目を抽出することをその目的とした。
- 詳細調査では、基礎調査に基づいて抽出した環境変化の項目（【図表3】）について、より詳細な調査を行い、将来の情報セキュリティ政策の検討や企画立案のための基礎資料を得ることをその目的とした。

【図表2】調査の流れと概要



【図表3】調査項目

（調査の対象とした環境変化）

No.	環境変化	各調査の対象	
		基礎調査	詳細調査
1	クラウド	○	
2	スマートフォン／タブレット端末	○	
3	BYOD	○	
4	リモートメンテナンス	○	
5	M2M	○	○
6	ビッグデータ	○	○
7	スマートシティ・スマートコミュニティ	○	(*)○

(*)特に中心的に採り上げた項目

3. 基礎調査結果（1/4）

重要インフラ分野における現状（環境変化の導入状況）

■ アンケート調査結果

○重要インフラ分野へ導入が進んでいる環境変化は、「リモートメンテナンス」「クラウド」「スマートフォン・タブレット端末」である（【図表4】参照）。

○また、重要システムへの導入率が高い環境変化は、「M2M」「リモートメンテナス」「クラウド」「ビッグデータ」である（【図表5】参照）。

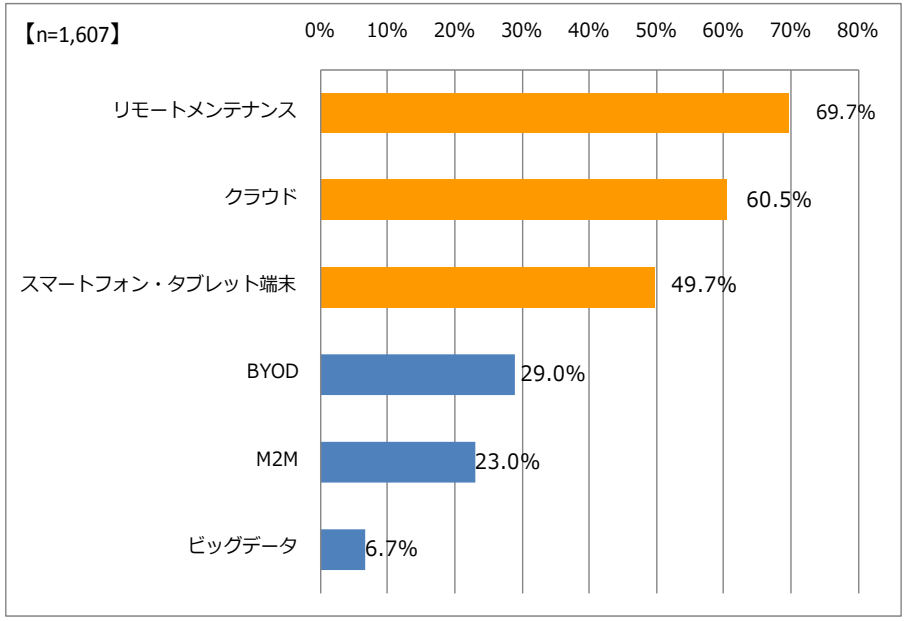
○上記のことから、重要インフラ分野では「リモートメンテナンス」が導入率も高く、重要システムでも多く利用されていると言える。

■ ヒアリング調査結果

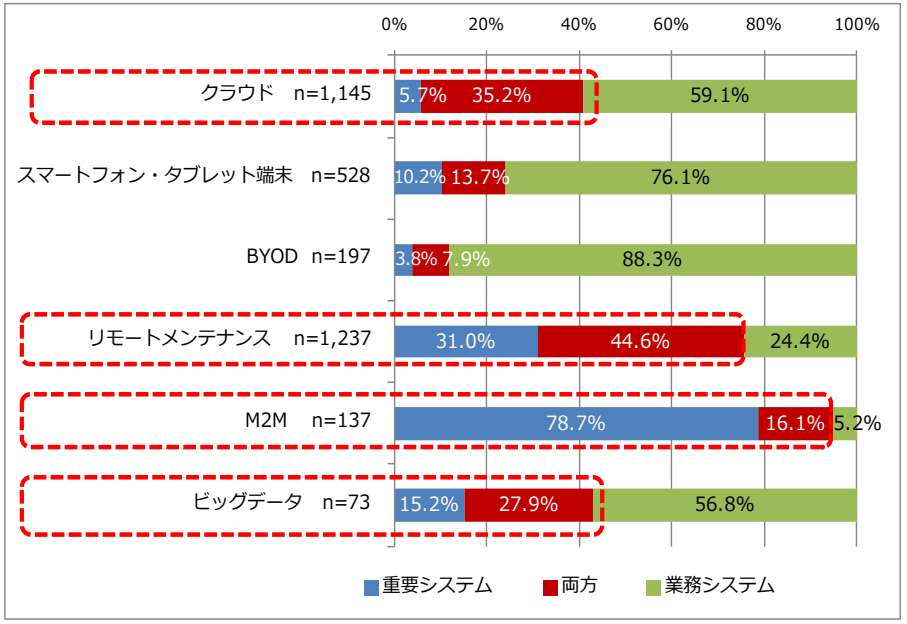
○「スマートフォン・タブレット端末」「ＢＹＯＤ」の普及は大きな流れであり、重要インフラ分野でも大きなツールになることが指摘されている。

○また、今後重要インフラサービスを大きく変えるものとして、「M2M」「ビッグデータ」「スマートシティ・スマートコミュニティ」が指摘されている。

【図表4】導入率の高い環境変化



【図表5】重要システムへの導入状況



3. 基礎調査結果（2/4）

重要インフラ分野における現状（情報セキュリティ対策の状況）

■ アンケート調査結果

○重要インフラ分野における環境変化毎の情報セキュリティ対策には、ばらつきが見られる（【図表6】参照）。

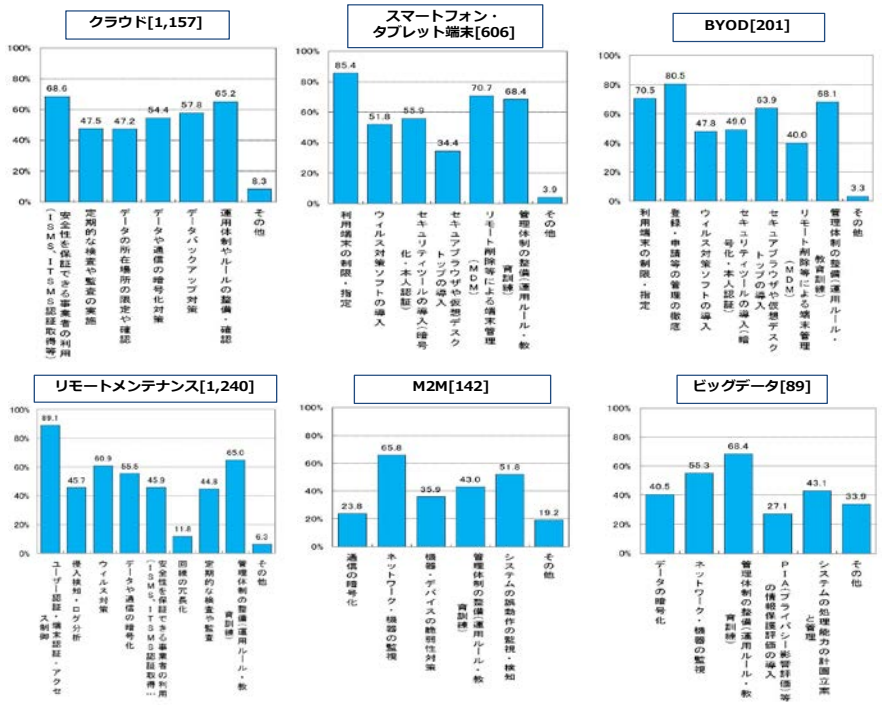
○また重要インフラ事業者では、環境変化個々の脅威や対策を十分に把握しているとは言えない状況にある（【図表7】参照）。特に「ビッグデータ」「M2M」「BYOD」といった重要インフラ事業者で導入率が低いものについて、十分に把握できていない傾向にある。

■ ヒアリング調査結果

○環境変化毎の情報セキュリティ対策は重要インフラ分野毎に異なっていることや環境変化毎のリスクに応じた情報セキュリティ対策の検討の必要性が指摘されている。

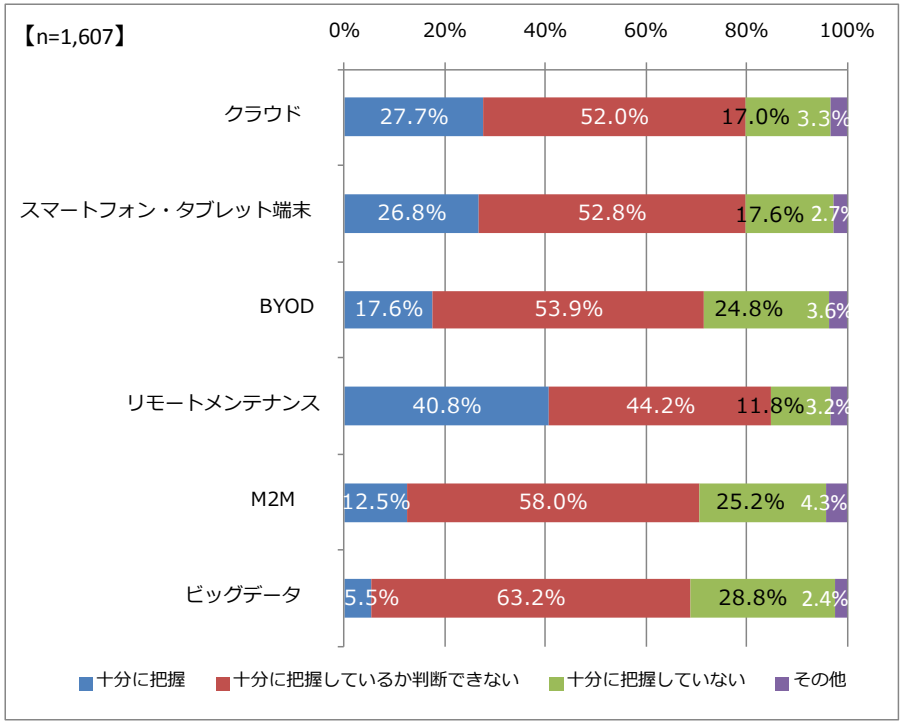
○また、「クラウド」「M2M」「スマートシティ・スマートコミュニティ」におけるサイバー攻撃のリスクが指摘されている。大量のセンサーネットワークによるリスクの増大のほか、自動制御やサービスの連携等、高度・複雑化によるリスクの増大や変質が懸念されており、利用方法や情報セキュリティ対策等は、今後議論が高まると予想される。

【図表6】環境変化毎の情報セキュリティ対策の状況



[ ]内の数値は、各環境変化に対して「導入している」「導入を予定している」「導入に向けて検討中（または検討予定）」の回答数

【図表7】環境変化毎の脅威・対策の把握状況



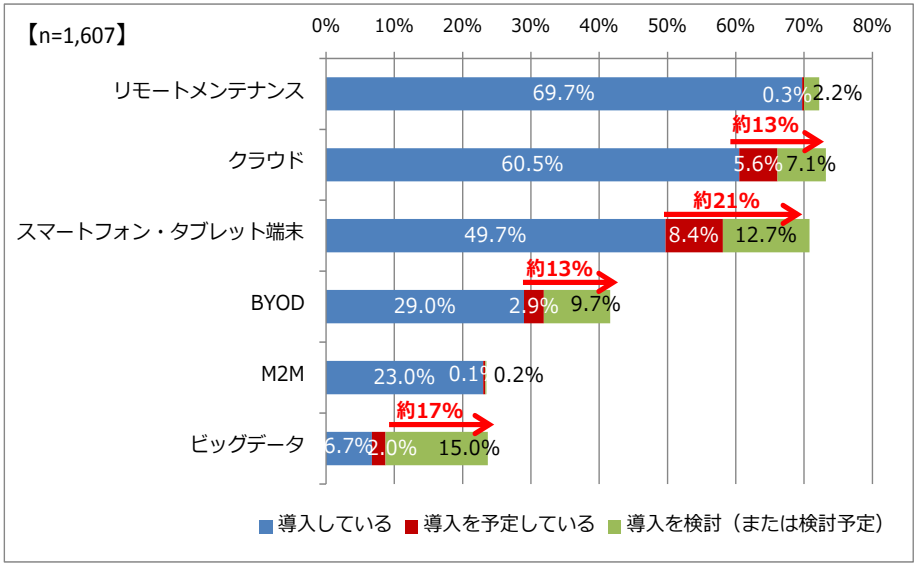
3. 基礎調査結果（3/4）

将来想定される環境変化と新たな脅威やリスク①

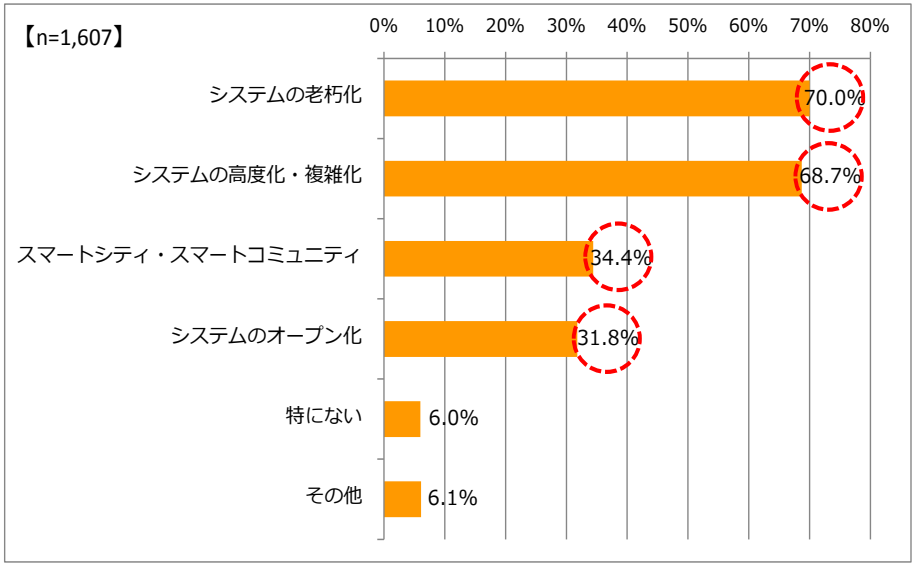
■ アンケート調査結果
○重要インフラ分野において、今後導入が進むと予測される環境変化は「クラウド」「スマートフォン・タブレット端末」「BYOD」「ビッグデータ」である（【図表8】参照）。
○また、重要インフラ分野における今後の脅威として「システムの老朽化」「システムの高度化・複雑化」「スマートシティ・スマートコミュニティ」「システムのオープン化」への意識が高い状況にある（【図表9】参照）。

■ ヒアリング調査結果
○「スマートシティ・スマートコミュニティ」が今後の環境変化として注視されている。
○また、「クラウド」「M2M」「ビッグデータ」といった環境変化の融合による「スマートシティ・スマートコミュニティ」といった新たな社会インフラの登場による新たな脅威の発生が予測されている。
○今後の導入過程において具体的な脅威やリスクの把握と設計段階から情報セキュリティ要件検討の必要性が指摘されている。

【図表8】今後導入が見込まれる環境変化



【図表9】今後の脅威

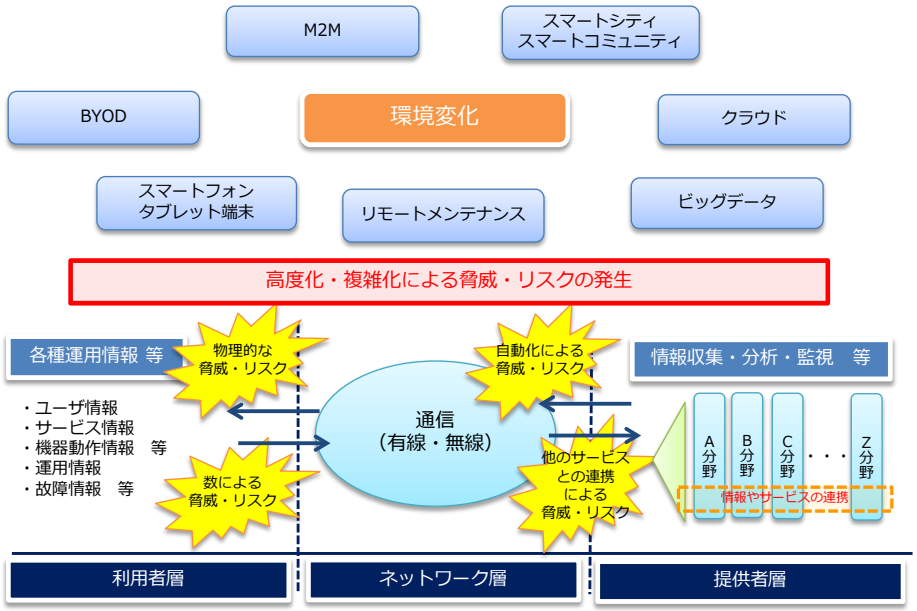


3. 基礎調査結果（4/4）

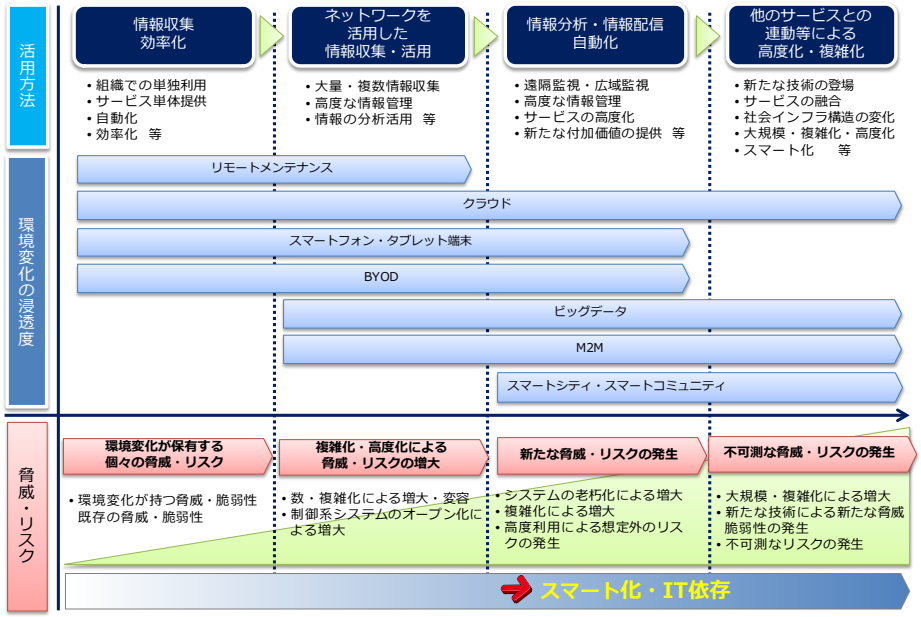
将来想定される環境変化と新たな脅威やリスク②

- 基礎調査から、環境変化に伴って発生する新たな脅威・リスク及び将来予測される環境変化による新たな脅威・リスクの例は、下図のとおりである（【図表10】【図表11】参照）。
- 今後は環境変化の進展とICTの高度利用によって、より効率的で利便性の高いサービスが提供されていくだけでなく、スマートシティ・スマートコミュニティといった新しい社会インフラの構築によってさまざまな連携が進むと想定される。そこには、新たな重要インフラとなり得る新規事業の登場や重要インフラ分野間の相互依存性の変化なども視野に入れる必要がある。
- そのような将来の社会構造の変化を想定したとき、ICTの高度化・複雑化による新たな脅威・リスクの発生やリスクの質が変質する可能性があることに十分留意する必要がある。この点に留意しながら、重要インフラサービスへの導入・拡大・波及が予測される環境変化への継続的な調査やリスクマネジメント等の取り組みが必要である。

【図表10】環境変化による脅威・リスクの発生の例



【図表11】将来予測される環境変化と脅威・リスクの例



4. 詳細調査結果（1/2）　スマートシティ・スマートコミュニティの全体像

■ スマートシティ・スマートコミュニティにおいて、導入が進んでいるエネルギーマネジメント分野を中心に調査を行った。

<現状>

○ 電力系統からなる供給側と、ICTを活用した地域エネルギーマネジメントシステム（地域EMS／CEMS）で構成される需要側との相互調整により最適化を図り、効率的な電力活用を実現することを目指している。

○ 地域EMS／CEMSは、地域における発電設備、ビルにおけるエネルギーマネジメントシステム（BEMS）、住宅におけるエネルギーマネジメントシステム（HEMS）等によって構成される。

○ それぞれの機能や役割は、立場によって定義や解釈が異なっている点に留意が必要である。

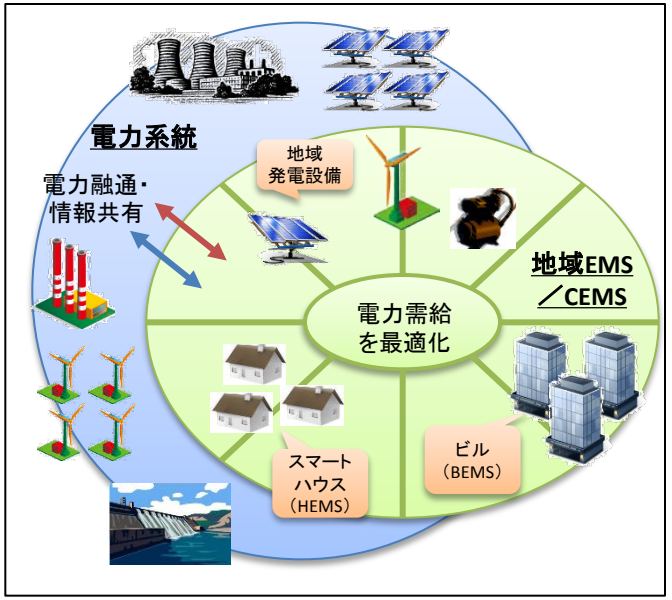
<将来像>

○ 現段階では、スマートシティ・スマートコミュニティにおけるエネルギーマネジメント分野の将来における全体像を確認することが出来なかった。

○ 今後、既存の重要インフラ事業者だけでなく、それ以外の事業者も含め、多様なプレイヤーがスマートシティ・スマートコミュニティを主導していくものと考えられる。

○ ヒアリング対象者からは、普及・発展を加速する要素として次の事項が挙げられた。

【図表12】調査対象としたスマートシティ・スマートコミュニティ（エネルギーマネジメント分野）のイメージ



【図表13】スマートシティ・スマートコミュニティ（エネルギーマネジメント分野）の普及・発展を加速する要素

インフラ整備により起こる変化	・スマートメーターの普及による家庭における電力利用情報の流通と新規サービスの展開 ・ビルやビル群のエネルギー管理の効率化
法規制の見直しにより起こる変化	・スマートメーターより得られる情報の取扱いルールの整備 ・電力小売自由化、発送電分離等の電力システム改革、それによる新電力（PPS）等の新規参入と淘汰、既存発電設備の用途拡大など。
技術革新により起こる変化	・蓄電技術の向上による地域エネルギーマネジメントシステムの自律性の向上、生産＝消費の概念の変化 ・エネルギーマネジメントシステム等で情報をやりとりするための安全なプロトコルの普及
その他	・オフィスビルの建て替え等による設備の更新により省電力化が進む

4. 詳細調査結果（2/2）スマートシティ・スマートコミュニティの情報セキュリティ上のリスク

- スマートシティ・スマートコミュニティにおけるエネルギーマネジメント分野においては、多様な事業者が同一のネットワークやプラットフォームに接続されること等により、情報セキュリティ上の問題点（リスク）が発生し、安定的な電力供給に支障をきたすおそれがある。
- スマートシティ・スマートコミュニティに関連する事業者や団体は、ITが機能不全に陥った場合でも国民生活や社会経済活動への影響を最小限に抑制するため、情報セキュリティ対策を含めた必要な準備の検討と実施を図ることが重要である。

【図表14】想定される情報セキュリティ上のリスクと重要インフラサービスへの影響

リスク源	情報セキュリティ上の問題点（リスク）	重要インフラサービスへの影響（例）
○多様な事業者が同一のネットワークやプラットフォームに接続 ○HEMS・BEMS・CEMS等を通じてシステムや機器の制御が可能 ○アグリゲーター等の有するシステムに電力利用に関する情報が集約 ○スマートメーターなどの重要な情報が流通する機器が利用者の手の届く場所に設置	○情報セキュリティ基準の不統一や責任分界点があいまいになるリスク ○制御システム等への不正アクセスや不正操作のリスク ○CEMS等の基盤設備における単一障害点としてのリスク ○メーター情報などの漏えい・改ざんのリスク ○家庭やビルにおける端末設備の物理的・論理的な破壊・変更・窃取リスク	○計測データの改ざんによる利用料金の誤請求・不正請求 ○電力需要の予測違い、それによる電力供給の不安定化や不足、途絶 ○発電設備への直接的な操作による電力の過供給による電力設備の破壊、電力供給の不安定化や不足、途絶 ○上述の結果引き起こされる事象による社会的混乱 など

スマートシティ・スマートコミュニティにおける情報セキュリティ上の今後の取り組みの方向性

①「システム」としての情報セキュリティ対策の確立　②制御システムとITシステムの情報セキュリティ対策のバランスの確保
③流通する情報の取扱いルールの明確化　④客観的な情報セキュリティ基準の整備
⑤重要インフラ事業者の範囲の見直しについての継続的かつ具体的な検討