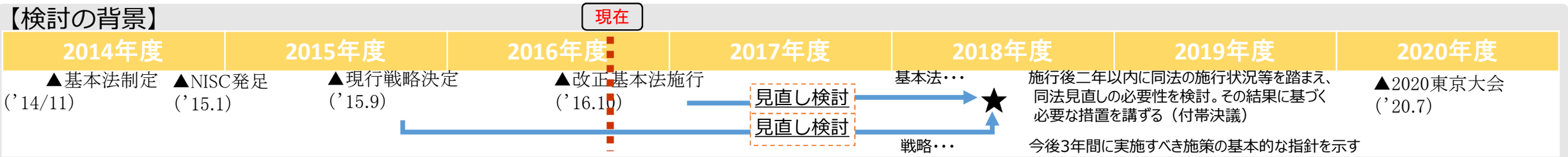
2020年及びその後を見据えたサイバーセキュリティの在り方について

資料2

【検討の背景】



◆ サイバーセキュリティ戦略の期間（～’18年9月）及び改正基本法の見直し期限（～’18年10月）まで1年余り

◆ 2020年東京大会に向けた抜本的対策を見据えた取組の必要
（当該取組はその後も見据えたもの）

【脅威の変化】

脅威の一層の複雑化
- 攻撃手法の高度化・大規模化
- 攻撃の「サービス化」
- 重要インフラのIT化の進展

防護対象の拡大
- 防護対象の面的増加
- マイナンバーの利活用の拡大
- 先端技術保有者への脅威の増大

脅威のグローバル化
- IoT機器の指数関数的増大と拡散
- 同時多発的なグローバルなサイバー攻撃等の増加

2020年及びその後に向けて更なる取組が必要

【課題と検討事項（例）】

IoTセキュリティの強化

◆ セキュアなIoTシステムの実現
◆ 日本発技術の開発・普及

（検討事項例）
- ✓ IoTｾｷｭﾘﾃｨ対策の官民連携体制強化
- ✓ IoTｾｷｭﾘﾃｨの国際標準化の推進　等

国際対応の強化

◆ 米国等との情報共有・連携の強化

（検討事項例）
- ✓ 先進国等との脅威情報等の共有・連携の強化
- ✓ 日本発製品・サービスの海外展開支援
- ✓ 途上国への政府開発援助等を通じた支援　等

重要インフラ等に関する取組強化

◆ 検知・判断・防御体制（重要ｲﾝﾌﾗ等）の強化
◆ 危機管理体制との連携強化

（検討事項例）
- ✓ 重要ｲﾝﾌﾗ等の障害・事故、脅威情報　の総合的な情報共有　（バーチャルサイバー脅威情報集約センター構築、情報共有システム・ホットライン構築）
- ✓ 最新技術を活用した政府機関等の監視システムの高度化
- ✓ 警戒体制の整備　（深刻度の場合分け・警戒レベルの設定）
- ✓ 危機管理体制との連携強化　（物理ｾｷｭﾘﾃｨに連動した緊急対応計画の策定等）　等

その他の主体に関する取組強化

◆ 地方公共団体における対策の一層の促進
◆ 研究開発法人、大学法人等における対策の促進

（検討事項例）
- ✓ 地方公共団体のｾｷｭﾘﾃｨ水準向上支援
- ✓ 先端技術保有者（大学等）のｾｷｭﾘﾃｨ水準向上支援　　等

東京ｵﾘﾝﾋﾟｯｸ・ﾊﾟﾗﾘﾝﾋﾟｯｸ競技大会等に向けた対策の強化

◆ 2020東京ｵﾘﾊﾟﾗ大会を見据えた対処体制の強化

（検討事項例）
- ✓ オリパラ対処調整ｾﾝﾀｰの整備、重要ｲﾝﾌﾗ事業者のﾘｽｸ分析の促進、十分な演習・訓練の実施　　等

連　携

（参考）
サイバーセキュリティ戦略

1 サイバー空間に係る認識
2 目的
3 基本原則
4 目的達成のための施策
- 経済社会の活力の向上及び持続的発展
- 国民が安全で安心して暮らせる社会の実現
- 国際社会の平和・安定及び我が国の安全保障
- 研究開発の推進、人材の育成・確保

5 推進体制

【今後の予定】

2017年1月25日	戦略本部（第11回）	検討方針等
今年度末目途	戦略本部（第12回）	方針の骨格の決定
来年度夏頃	戦略本部（第13回）	方針の決定
～2018年6月	可能な施策から段階的に実施（1年以内の完全実施）	

この間、有識者会合の開催（随時）