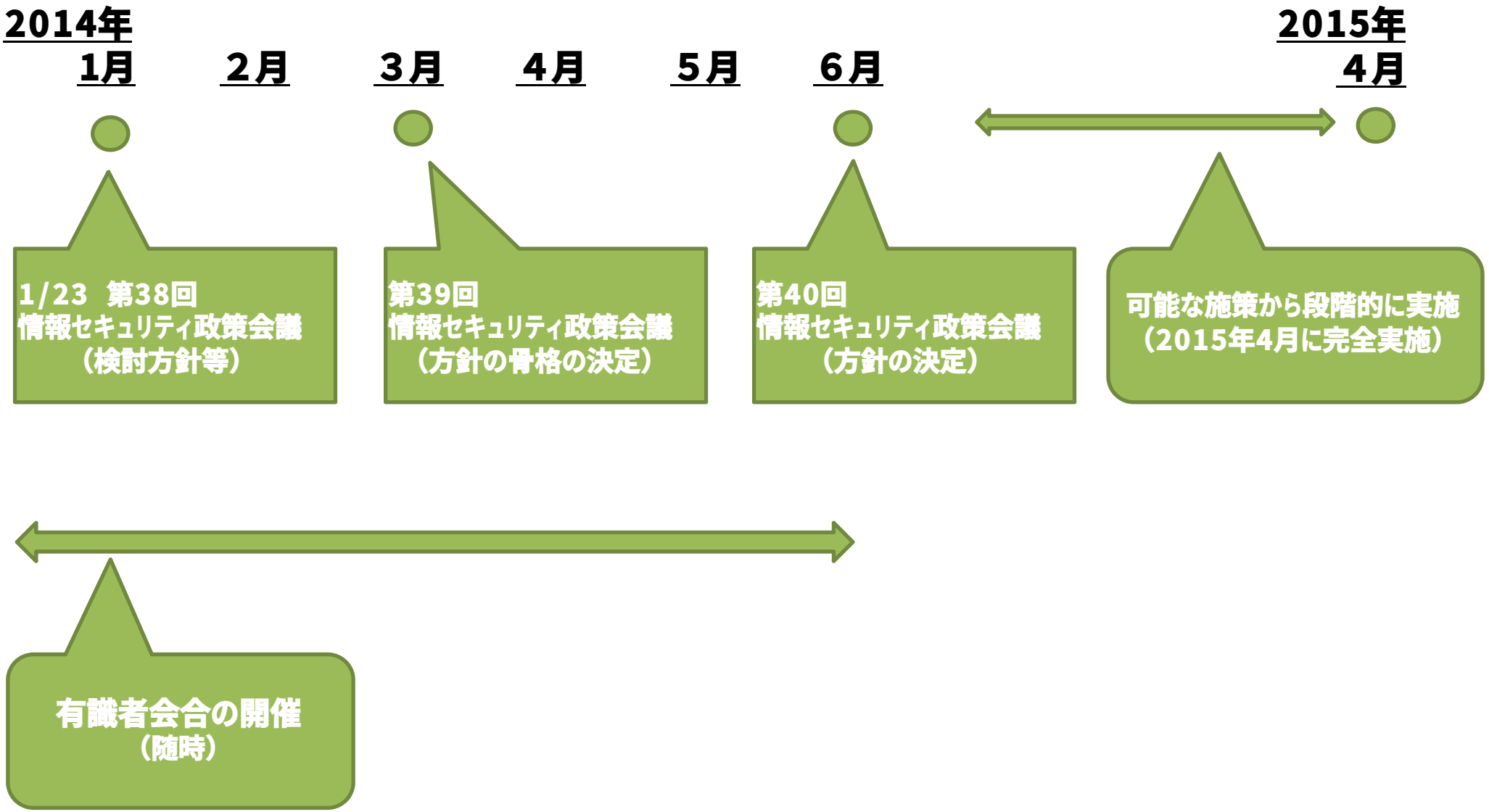
NISCの機能強化に関する検討について

資料6

サイバー脅威の高度化・深刻化	NISCの機能強化の方向性	機能強化に向けた検討事項
サイバー脅威の甚大化 ●標的型メール攻撃など機微情報や技術情報への攻撃の急増 ●重要インフラへの攻撃の増加	**能動的な役割の強化** ●NISCの知見が各府省等に活用される仕組みの構築 ●東京オリンピック・パラリンピックにも備え先行的に政府の体制強化	●GSOCの機能の強化 ●重大なインシデントに関する原因究明など事後調査機能の強化 ●専門的人材の配備・育成（分析研究員の配置等）
サイバー脅威の拡散 ●スマートフォンの普及等に伴うリスクの拡散 ●自動車、制御系システム等へのリスクの高まり	**横串的機能の強化** ●各府省等のセキュリティ水準の向上に向けたNISCの積極的貢献 ●関係省庁のセキュリティ政策間の組織・分野横断的な実効性の確保	●各府省等の情報システムに関するセキュリティ監査機能の強化 ●ITセキュリティ投資に関する評価機能の強化（政府CIOと連携） ●関係省庁のセキュリティ政策間の総合調整機能の強化（政府CIOと連携）
サイバー脅威のグローバル化 ●国境を越えたサイバー攻撃等の急増 ●国家機関の関与が疑われる攻撃の顕在化	**情報集約・国際連携機能の強化** ●脅威情報等の集約・共有化の促進 ●国際連携取組方針に基づく米、EU、ASEAN等との連携強化	●政府機関・重要インフラのインシデント情報の集約機能の強化 ●官民にまたがる複数の国際的窓口機能の在り方の整理 ●政府間連携のための人員拡充

検討スケジュール等


2014年
1月
2月
3月
4月
5月
6月
2015年
4月
1/23　第38回
情報セキュリティ政策会議
（検討方針等）
第39回
情報セキュリティ政策会議
（方針の骨格の決定）
第40回
情報セキュリティ政策会議
（方針の決定）
可能な施策から段階的に実施
（2015年4月に完全実施）
有識者会合の開催
（随時）

【参考】 NISCの機能強化に向けた政府方針

サイバーセキュリティ戦略（平成25年6月情報セキュリティ政策会議決定）

NISCについては、世界を率先する強靭で活力あるサイバー空間を構築するための我が国の司令塔として、機能強化を行う。具体的には、**GSOCの抜本的な強化**を図るとともに、サイバー攻撃に関する**インシデントに関する情報等の集約**、サイバーセキュリティに関する**国内外の動向等の実態及び政府の関連施策の現状に関する分析・周知**、政府機関及び独立行政法人等の**関連専門機関等に分散している各種機能の有機的な連携による動的な対応**等を強化する。その際、**国際的なインシデント対応における我が国の窓口となるCSIRT機能**の在り方についても併せて検討する。

以上を踏まえ、NISCについては、**専門職員の採用や育成等の人事管理による人材の確保**や**権限等の必要な組織体制**を整備することにより、2015年度を目途として「サイバーセキュリティセンター」（仮称）に改組するものとする。

国家安全保障戦略（平成25年12月国家安全保障会議決定・閣議決定）

サイバーセキュリティを脅かす不正行為からサイバー空間を守り、その自由かつ安全な利用を確保する。また、国家の関与が疑われるものを含むサイバー攻撃から我が国の重要な社会システムを防護する。このため、**国全体として、組織・分野横断的な取組を総合的に推進**し、サイバー空間の防護及びサイバー攻撃への対応能力の一層の強化を図る。

そこで、**平素から、リスクアセスメントに基づくシステムの設計・構築・運用、事案の発生の把握、被害の拡大防止、原因の分析究明、類似事案の発生防止**等の分野において、**官民の連携を強化**する。また、**セキュリティ人材層の強化、制御システムの防護、サプライチェーンリスク問題への対応**についても総合的に検討を行い、必要な措置を講ずる。

さらに、国全体としてサイバー防護・対応能力を一層強化するため、**関係機関の連携強化と役割分担の明確化**を図るとともに、**サイバー事象の監査・調査、感知・分析、国際調整等の機能の向上**及びこれらの任務を担う**組織の強化**を含む各種施策を推進する。

かかる施策の推進に当たっては、幅広い分野における**国際連携の強化**が不可欠である。このため、**技術・運用両面における国際協力の強化**のための施策を講ずる。また、**関係国との情報共有の拡大**を図るほか、サイバー防衛協力を推進する。