別添資料3

共同閣僚声明の概要

原則 （「セッション1」において議論）

- 信頼性の高いサイバー空間を育むいかなる手段も、情報の流通、相互運用性及び経済的繁栄を継続して促進すべきものであり、また、インターネットが技術的に円滑に機能することを損なわないものであるべき
- 規制手段が導入される際は、情報の流通の維持と経済活動の促進のため、十分な配慮がなされるべき
- 個々のインターネットの利用者は、自己規制を含むサイバーセキュリティに関するリテラシーを高めることを奨励されるべき
- 政策立案機関や規制機関は、サイバー脅威やリスクに効果的かつ迅速に対応するため、民間部門と連携すべき

Ⅰ 安心・安全なビジネス環境の構築 （「セッション3」において議論）

- ISMS[注1]等を通じた官民のサイバーセキュリティ水準の向上

  注1 Information Security Management Systemの略。組織（企業、部、課など）における情報セキュリティ管理するための仕組み。これに関する研修を実施。更に、制御システムセキュリティ分野にも対象を拡大。

- シーサート CSIRT[注2]等の関係省庁間の協力・連携の促進

  注2 Computer Security Incident Response Teamの略。セキュリティ上の問題に関する報告を受け、調査・対応する組織。

Ⅱ　安心・安全な情報通信ネットワークの構築　（「セッション２」において議論）

- ボットネット対策やスパム対策に関する情報交換などネットワークセキュリティの強化
- 「サイバー攻撃予知即応プロジェクト（PRACTICE[注3]）」及び「感染警告[注4]」から成るセキュリティにおける技術協力の強化（JASPER[注5]）

注3 Proactive Response Against Cyber-attacks Through International Collaborative Exchangeの略。サイバー攻撃に関する情報を収集・分析の上、情報共有を行い、サイバー攻撃発生の予知・即応を可能とする技術を確立するプロジェクト。総務省予算（H23年度からH27年度）で現在までに15億円で研究開発中。現時点で、インドネシア、タイ、マレーシアからサイバー攻撃観測データの提供を受けている。

注4 独立行政法人情報通信研究機構（NICT）が2012年6月に国内でサービスを開始。

注5 Japan-ASEAN Security PartnERshipの略。ASEAN各国向けのセキュリティ対策に関する総合的な技術協力プロジェクト。注3及び注4の2つのプロジェクトの総称。

- 研究者交流やインターネットサービスプロバイダ（ISP）間の協力等の技術的専門知識の交換

Ⅲ　サイバーセキュリティ能力の強化　（「セッション４」において議論）

- サイバーセキュリティ戦略における協力の促進（重要インフラ防護、官民協力、ICT分野における事業継続計画、オンライン上の弱者の保護、クラウドコンピューティングセキュリティ及びスマートフォンセキュリティを含む）
- 「日・ASEANサイバーセキュリティ人材育成イニシアティブ」[注6]の開始

注6　専門家派遣等によるASEAN各国政府職員向けの戦略的なセキュリティ研修の取組み。

- インシデントへの即応及び情報共有を促進するための仕組みの構築（サイバー演習など）
- 日本とASEAN各国間の共同意識啓発活動の促進