「サイバーセキュリティ 2013（案）」に関する意見書

内閣官房情報セキュリティセンター（基本戦略担当）殿

H25.6.24

所 属	ソフトバンク BB 株式会社 ソフトバンクテレコム株式会社 ソフトバンクモバイル株式会社	（ふりがな） 氏 名	（そん まさよし） 孫 正義
（ふりがな） 住 所	（とうきょうと みなとく ひがししんばし） 〒105-7304 東京都港区東新橋 1-9-1 （ソフトバンク BB 株式会社） 〒105-7316 東京都港区東新橋 1-9-1 （ソフトバンクテレコム株式会社） 〒105-7317 東京都港区東新橋 1-9-1 （ソフトバンクモバイル株式会社）		
連絡先	（ふ り が な） 連絡担当者氏名： 電話： FAX： e-mail：		

該当箇所	• P.16 ① 政府機関等における対策 2）サイバー攻撃への対処態勢の充実・強化【CYMAT と CSIRT 等との連携強化や訓練等による対処態勢の構築・強化】（ク）「新たなサイバー攻撃に対する情報セキュリティ防御モデル」の検討及び演習の実施 総務省において、サイバー攻撃の解析及び防御モデルの検討を行い、官民参加型の実践的な防御演習を行う。（総務省） （ケ）大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等（内閣官房及び関係府省庁）（P.27 再掲） 内閣官房において、関係府省庁と協力し、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を実施し、当該結果を踏まえた検討を行うこと等により、大規模サイバー攻撃事態等が発生した際に、「緊急事態に対する政府の初動対処体制について（2003 年11月21日閣議決定）」、「大規模サイバー攻撃事態等への初動対処について（2010 年3月19日内閣危機管理監決裁）」等に基づき官民が連携して的確な対応を行うことができる態勢を整備する。また、上記訓練は次年度以降も継続して実施する。 • P.24 ② 重要インフラ事業者等における対策 【重要インフラ障害に対する連携対応能力の強化】（ス）分野横断的演習の実施（内閣官房及び重要インフラ所管省庁） 内閣官房において、重要インフラ所管省庁、重要インフラ事業者等、セプター等の協力を得て、具体的な IT 障害発生を想定した演習シナリオの作成とそれに基づく分野横断的な演習を実施し、各事業者等の BCP の改訂等に資する課題を抽出する。

	（セ）個別分野におけるサイバー演習（総務省及び経済産業省） 経済産業省において、重要インフラの制御系の情報セキュリティ対策のため、今後、実際にサイバー攻撃が発生することを前提としたサイバー演習を実施し、制御システムのセキュリティ評価及びセキュリティ対策に関する知見を蓄積し、我が国の制御システムのセキュリティ対策に繋げる。
意見内容	• サイバー演習等を実施する際には、事業者に過度の負荷・負担を強いることがないよう配慮をすることが必要と考えます。
理由	• 安全に関する重要情報の収集及び高度な解析を実施すること、また、その収集情報や解析情報及び結果・対策等を関係する事業者等への共有し、事業者の対策に活用することは非常に重要と考えます。 • それら情報を用いた演習等を通じ、重要インフラ事業者等におけるノウハウ蓄積を目的としたシナリオ作成及びその精度向上のため、PDCA サイクルを実施していくことは、事業者における相当な負荷・負担が必要となることも想定されます。

該当箇所	• P.21 ② 重要インフラ事業者等における対策 【新たな「行動計画」の策定】（ア）新たな「行動計画」の策定（内閣官房及び重要インフラ所管省庁） 内閣官房において、重要インフラ所管省庁と協力し、重要インフラの防護を強化するため、重要インフラ事業者等及び政府機関との間における情報共有の仕組みや重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について検討を行うほか、「重要インフラの情報セキュリティ対策に係る第2次行動計画」の見直しを実施した上で、新たな「行動計画」を策定する。 （ウ）内閣官房において、重要インフラ所管省庁の協力を得つつ、「安全基準等」の整備浸透状況について以下の調査を行う 〈重要インフラ分野における調査〉 「安全基準等」の分析・検証及び改定等の実施状況、攻撃動向や情報システムに係る環境変化への対応状況の把握及び検証を行い、結果を公表する。 〈重要インフラ事業者等に対する調査〉 「安全基準等」の浸透状況に係る調査を行い、結果を公表する。また次年度の調査のための企画・準備を行う。
意見内容	• 国の安全に関する重要な情報について、収集及び高度な解析を実施することは非常に重要です。また、その収集情報や解析情報及び結果・対策等を関係する事業者等への共有し、事業者の対策に活用することも非常に重要と考えます。 • 事業者間の情報共有においては、個人情報・秘密情報に配慮し、事業者が特定できないよう匿名化を実施・徹底して頂きたいと考えます。 • また、共有の形態については、事業者間で直接実施するのではなく、事業者以外の中立的な第三者を経由しての共有が望ましいと考えます。

理由	• 事業者間で共有される情報には、各社の経営情報が含まれる可能性が高いため、事業者が特定できないよう匿名化が必須と考えます。 例）事業者と利用機器、請負業務、費用等の特定や関係性がわからないようにすること

該当箇所	• P.46 ③ 企業・研究機関等における対策 【インシデントの認知・解析機能の向上】（ノ）情報セキュリティ目的の通信解析の可能性等関連制度の柔軟な運用（総務省） 総務省において、情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について、可能な範囲で速やかに一定の結論を得るよう、サイバー攻撃等の実態、これに対する現行の取組状況等の実態把握に努めるとともに、情報セキュリティを目的とした通信解析における課題の洗い出し等を行う。 • P.50 ⑤ サイバー空間の犯罪対策 【事後追跡可能性の確保】（サ）ログの保存の在り方（警察庁及び総務省） 警察庁及び総務省において、相互に連携しつつ、サイバー犯罪に対する事後追跡可能性を確保するため、可能な範囲で速やかに一定の結論を得るよう、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討する。 特に、通信履歴の保存については、通信の秘密との関係、セキュリティ上有効な通信履歴の種類、保存する通信事業者等における負担、海外でのログ保存期間、一般利用者としての国民の多様な意見等を勘案した上で、サイバー犯罪における捜査への利用の在り方についての検討を行う。
意見内容	• 「通信履歴の保存」については、「通信履歴の保存」の必要性及び有効性を慎重に議論する必要があると考えます。具体的には、今回の議論は匿名統計化をされたデータの扱いとは異なることから、事前に十分な法的議論を経る必要があると考えます。よって、「事前に法的な議論をオープンな環境で実施した上で」の加筆を求めます。 • また、「通信履歴の保存」が必要と判断された場合においても、法令等の改正やガイドライン等の整備といったステップを踏む必要があると考えます。 • 更に、実施する場合においても、「通信履歴の保存」は、通信事業者に多大なコスト負担・運用負荷がかかることから、対象範囲・対象期間等の条件については、事業者に過度の負担となることのないよう配慮が必要と考えます。
理由	• 今回の議論における通信履歴に関しては、サイバー攻撃等への対処として、個人を特定することが想定されます。これは、憲法及び電気通信事業法にて保障されている通信の秘密を侵す可能性が非常に高いものと考えます。 • よって、検討を実施するに当たり、「通信履歴の保存」の必要性及び有効性を慎重に

	議論する必要があると考えます。また、「通信履歴の保存」が必要と判断された場合においても、法改正及び基準等のガイドライン等の整備のステップを踏む必要があると考えます。 • また、「通信履歴の保存」は、通信事業者に多大なコスト負担・運用負荷がかかることから、通信事業者の意見を十分にヒアリング・把握したうえで検討頂きたいと考えます。 • 加えて、全ての通信履歴の保存を行うのではなく、サービス等の特性に準じて優先順位の整理を行い、必要と考えられるものを保存するという考え方が必要です。

該当箇所	• P.37 ④ サイバー空間の衛生 【普及啓発】（コ） 各種メディア等を通じた普及・啓発の推進（内閣官房、警察庁、総務省、経済産業省及び文部科学省） c） 総務省及び文部科学省において、各府省庁と協力し、保護者、教職員及び児童生徒を対象に、子どもたちのインターネットの安心・安全な利用に向けた啓発のための講座（「e-ネットキャラバン」）を、通信関係団体等と連携しながら全国規模で実施する。 d） 総務省において、各府省庁と協力し、スマートフォン等が急速に普及していることを踏まえ、利用者に対して、スマートフォン等の情報セキュリティ対策について総合的な普及・啓発を推進する。
意見内容	• 普及・啓発活動を実施してくことは非常に重要なことであり事業者も日々努力をしていますが、事業者に過度の負荷・負担を強いることがないよう配慮をすることが必要と考えます
理由	• 全国規模や総合的な普及・啓発活動を継続的に実施していくためには、事業者における相当な負荷・負担が必要となることも想定されます。

該当箇所	• P.68 （カ） スマートフォン等におけるフィルタリングの在り方の検討（総務省及び経済産業省） 総務省及び経済産業省において、スマートフォン等に対応したフィルタリングの改善に向け、関係事業者との調整に取り組む。 • （キ） スマートフォン時代における利用者情報保護に関する取り組みの推進（総務省） 総務省において、「スマートフォンプライバシーイニシアティブ」（「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」提言）に示された「スマートフォン利用者情報取扱指針」に基づき、業界ガイドライン及びアプリケーションのプライバシー・ポリシーの作成促進及び利用者に対する情報提供・周知啓発等、総合的な利用者保護に関する取組みを推進するとともに、スマートフォンのアプリについて、一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みを構築する。

意見内容	• 一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みを構築することは重要なことと理解しますが、スマートフォンのアプリについては、一般社団法人電気通信事業者協会主導で、事業者対応基準（アプリケーション提供サイト運営事業者向けガイドライン）が策定・運用されています。 • 複数の仕組みが導入・運用された場合は、一般利用者の混乱も想定されることから、どの仕組みを推進していくのか等の整理が必要と考えます。
理由	• アプリケーション提供サイト運営事業者向けガイドラインは、アプリケーション提供サイトを運営する携帯電話事業者が、プライバシー及び情報セキュリティの観点から適切でないアプリケーションを提供サイトから排除し、アプリケーション提供サイトを適正に運用すること、利用者への周知・啓発を行うことを目的としています。

以上