「サイバーセキュリティ戦略（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

H25.6.4

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	• 2.基本的な方針 (3)各主体の役割 （P18～23）
意見内容	• 本項目においては、「各主体の役割」が規定されていますが、対処すべき対策や想定される攻撃等は「サービス」や「重要度」、「社会に対する責任」等によって変わってくるものと理解しています。従って、主体ごとに一つのルールを適用するのではなく、保護する対象に応じた適正な対処が可能となるよう、優先順位や対処レベル等の整理を行うべきと考えます。 • また、情報通信産業は、今後多くの新規事業者の参入も期待される分野であることから、過度な負荷・コスト負担を強いることのないよう配慮が必要と考えます。
理由	• ブロードバンド環境が普及している日本においては、多様な分野においてICTが活用されおり、今後も更なる発展が見込まれます。そのような環境下においては、情報システムや情報通信ネットワーク等のセキュリティを確保し、経済の発展、国民の安全・安心確保を実施してくことは非常に重要なことと理解しています。また、通信事業者として安心・安全のために日々努力をしているところです。 • しかしながら、情報システムや情報通信ネットワーク等は、スマートデバイス、M2M・センサーネットワーク、クラウドコンピューティングサービス等と多種多様であり、その活用先も電子商取引、医療、教育、交通、社会インフラ管理、行政等の多様な分野に及びます。 • その機能と分野によって対処すべき対策や想定される攻撃等は異なるものと考えられることから、その特性に応じ、適宜適切に対応することが重要と考えます。

	• サイバーセキュリティ戦略(案)に記載があるように、サイバー産業の活性化を行っていくには、新規事業者の参入が必要です。従って、事業者に過度の負荷・負担を強いることがないよう、例えば、最低限必要な基準等を策定し、追加処置はオプション方式とするような方法も一案と考えます。

該当箇所	• 2.(2)③ リスクベースによる対応の強化 (P17) サイバー攻撃に関するインシデントの認知・解析機能の向上、これらの機能の連携、情報共有の促進による脅威分析能力の高度化、各主体の CSIRT 間の連携や国際的な CSIRT 間連携の強化等が重要であり、これらによる動的対応力を通じ、リスクの性質を踏まえたリスクベースによる対応を強化することが必要である
意見内容	• 各主体の CSIRT 間の連携や国際的な CSIRT 間連携の強化等について賛同します。
理由	

該当箇所	• 3.(1)「強靱な」サイバー空間の構築 ①政府機関等における対策 【情報及び情報システムに係る情報セキュリティ水準の一層の向上】(P.26) 国の安全に関する重要な情報について、国以外の事業者による取扱いにおける情報セキュリティを強化する。こうした情報については、情報処理業務の外部委託、一般の調達及び補助事国の安全に関する重要な情報について、国以外の事業者による取扱いにおける情報セキュリティを強化する。こうした情報については、情報処理業務の外部委託、一般の調達及び補助事業等の場合における情報セキュリティ要件の担保が図られているが、これに加え、サイバー攻撃に関するインシデント情報の発注省庁等への報告及び事業者間の情報共有の促進を図る
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。併せて、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ついては、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	• 3.(1)①政府機関等における対策 【サイバー攻撃への対処態勢の充実・強化】(P.26) 具体的には、GSOC82 を抜本的に強化することとし、監視対象を一層拡大するととも

	に、監視対象先におけるインシデント情報の効果的な収集及び高度な解析を可能とするための技術や組織体制等を整備し、あわせて攻撃手法の分析結果等をリスク評価手法の強化に反映させる体制等を整備する。また、収集したインシデント情報や攻撃手法の分析結果等について、監視対象先となる省庁等の政府機関や、重要インフラ事業者等の関係機関と共有するための仕組みも整備する。
意見内容	• 国における収集したインシデント情報や攻撃手法の分析結果等について、重要インフラ事業者等の関係機関と共有するための仕組みも整備することに賛同します。 • 前述した通り、情報共有に当たっては事業者が特定できないよう匿名化を実施徹底すべきと考えます。
理由	• 事業者単位での対策では収集可能な情報数や対策に限界も考えられ、各種情報及び対策について、共有化を図ることは望ましいと考えます。 • また、前述の通り匿名化は必須と考えます。

該当箇所	• 3.(1)②重要インフラ事業者等における対策（P.28） 重要インフラ事業者等におけるリスク評価手法に基づく情報セキュリティ対策の重点化を図るため、各分野における直近の安全基準等の策定・変更状況及びリスク分析を通じて、分野横断的に講じることが望ましいリスクを洗い出し、安全基準等を策定するための指針の中に反映するプロセスを確立する。
意見内容	• 前述の通り 、重要インフラ事業者においても多様なサービスやシステムを保有していると考えられることから、一様に「重要インフラ事業者等」のセキュリティ対策を検討するのでなく、サービス等の特性に準じて優先順位や対処レベル等の整理を行うべきと考えます。
理由	• 前述の通りです。

該当箇所	• 3.(1)②重要インフラ事業者等における対策（P.28） 業種間での情報共有が難しい標的型攻撃に関する情報については、秘密保持契約に基づく情報共有体制を深化・拡充する。また、重要インフラ事業者等による事業所管省庁への迅速な報告、自主的判断に基づく事案対処省庁への通報及び関係機関との情報共有については、個人情報・秘密情報に配慮した上で促進する。
意見内容	• 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。

	• 但し、個人情報や通信の秘密については、違法性阻却事由となる基準を国が定めて頂くことが必要と考えます。
理由	• 事業者判断で実施した場合、基準がまちまちとなり、収集情報が情報価値として低下する懸念があります。

該当箇所	• 3.(1)②重要インフラ事業者等における対策（P.28） 重要インフラ事業者等とサイバー空間関連事業者との脆弱性情報や攻撃情報等の情報共有等による連携の促進、SCADA 等の制御系機器・システム等の調達・運用における国際標準に則った評価・認証導入の在り方の検討や、制御系機器・システムの評価・認証機関の設立に向けた取組を進めていく
意見内容	• 標準化等を推進することで、対策・運用等の効率化が図ることは重要なことと理解しますが、評価・認証を導入することにより自由競争が阻害されることのないように考慮することが必要と考えます。
理由	• 事業者は、各社の努力によりシステム構築や機器等の調達・運用を実施し、競争を実施しているところです。評価・認証基準を厳格化することで、競争原則が働かなくなる可能性を危惧します。

該当箇所	• 3.(1)③企業・研究機関等における対策（P.29） 上場企業におけるサイバー攻撃によるインシデントの可能性等について、競争条件の公平性等に配慮しつつ、事業等のリスクとして投資家に開示することの可能性を検討する。その際、関連情報の共有など開示するインセンティブを促すための仕組みの在り方についても併せて検討する。
意見内容	• 有価証券報告書等に記載する「事業等のリスク」に、サイバー攻撃に対するインシデントの可能性等の記載を検討される場合は、有価証券報告書の所管である金融庁殿と協議の上、進めて頂きたいと考えます。
理由	• 有価証券報告書の記載要領は、企業内容等の開示に関する内閣府令第三号様式にて定めているため、本様式の手当てが必要と考えます。

該当箇所	• 3.(1)④サイバー空間の衛生（P.31） 今後、マルウェアを配布する等の悪性サイト情報を蓄積するデータベースを構築し、悪性サイトにアクセスしようとする一般利用者に対する注意喚起等を、ISP 等により実施するための仕組みを構築し、悪性サイトの検知機能の強化などデータベースの機能の高度化を推進
意見内容	• 一般利用者に対する注意喚起については、事業者も日々努力をしていますが、注意喚起の仕組みに関しては、事業者のみではなく、官民一体となって推進していくことが必要と考えます。例えば、対処の判断基準等において、事業者判断が困難である場合、

	公的機関により判断を行う等の体制が考えられます。 • また、国民全体のリテラシー向上が必須となることから、学校においての教育や高齢者においては、自治体の指導・案内等も必要と考えます。
理由	• 事業者のみで推進を行う場合、対応判断等の基準に差分が発生し、利用者の理解度の差分や混乱が生じてしまう懸念等があります。

該当箇所	• 3.(1)⑤サイバー空間の犯罪対策（P.32） また、サイバーパトロールの強化やスマートフォン用アプリに係る被害防止対策の推進等による官民一体となったサイバー犯罪抑止対策を推進するとともに、民間事業者等への手口分析等の嘱託等による民間の知見の捜査等への活用を図る。
意見内容	• 前述の通り 、情報共有に当たっては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、国民全体のリテラシー向上が必須となることから、学校においての教育や高齢者においては、自治体の指導・案内等も必要と考えます。
理由	• 前述の通りです。

該当箇所	• 3.(1)④サイバー空間の衛生（P.31） 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検討する。 • 3.(1)⑤サイバー空間の犯罪対策（P.32） 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、海外でのログの保存期間、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検討する。
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。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の整備のステップを踏む必要があると考えます。 • また、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。 • 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。
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ると考えています。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。

	• 従って、検討を実施するにあたり、「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し、把握した上で検討頂きたいと考えます。

該当箇所	• 3.(2)「活力ある」サイバー空間の構築 ④リテラシー向上 (P38) スマートフォンへの移行に伴い、その利用率が大幅に拡大している SNS 等、スマートフォンの利用に関する効果的な対策等について、関係事業者等と協力しその確保を図る。さらに、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