（別紙１）

平成２７年度戦略的イノベーション創造プログラム（SIP）新規課題候補「重要インフラ等におけるサイバーセキュリティの確保」の研究開発計画（案）に関するご意見と考え方

No	ご意見	ご意見に対する考え方
1	サイバーセキュリティを実現できる方式原理を研究開発すべきである。そのような方式原理の例を挙げる。 1.　汎用OSも、標準化されたプログラミング言語も、標準化されたファイル形式も使用しない動作モードを持つシステム。 2.　通信相手ノードの地理的位置を即時に検出して、通信相手のリアルタイム認証をする。	ご意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
2	時宜を得た国としてまさに推進すべきプログラムと思いますが、成果の普及の点で、次の2点は課題と考えます。 ・計画案でも触れられているように、セキュリティ認証制度などへの取り込みにより、セキュリティ対策の導入を事業者等に促す（場合によっては必須とする）ような施策が必要と思います。 ・その際、SIPの開発成果が、民間の自助努力による開発成果の普及を、不要に圧迫することがないよう配慮が必要と思います。認証における必須要件を過度に限定しないなどの対応により、これは達成できるものと考えます。	ご指摘の点については、セキュリティ認証制度に関する今後の検討に当たっての参考とさせていただきます。
3	・研究開発計画（案）8ページの脚注で、「セキュリティ確認」の定義として、「真正性・完全性を確かめる。」と定義しているが、製造段階での（HW機能を含む）マルウェア機能等の定義されていない（不正機能を含む）「隠された機能」の混入を検出する「健全性」も確認すべきではないか。また、「セキュリティ確認」という用語は、本研究計画の中核的な概念であるので、本文中で、明確に定義すべきと考える。	ご指摘の「健全性」については、本計画案のなかでは「完全性」の概念に含めて記載しています。また、「セキュリティ確認」の定義については、原案どおり脚注に記載させていただきます。
4	・「研究開発」の成果が、将来的にガラパゴス化する危険性と、2020年にシステムとして実証するという目標を考えると、既存技術であっても、使える技術は使うという視点に立つべきであると考える。例えば、（2）研究開発項目(a1)では、TPM（Trusted Platform Module）などの既存技術の積極的な利用も検討していただきたい。	ご意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
5	・（2）研究開発項目(a1)では、機器を構成するMPU等の機能部品・能動部品レベルでの不正機能の混入検出するテスト技術開発も明記すべきであると考える。 ・同じく（2）研究開発項目(a1)で開発されるテスト技術は、「攻撃技術」の応用であるとの認識から、「新しい攻撃シナリオとその具体化」も公募対象に含めるべきと考える。	ご指摘の点については、テスト技術に関する研究開発機関の公募検討の参考とさせていただきます。攻撃手法を含めたテスト技術に関する研究開発提案はあり得ると考えています。
6	（2）研究開発項目(a4)で開発されるセキュリティ確認方法の適用先であるIoT機器や機能部品の場合、アフターマーケットの存在やIT機器・完成品とは異なる流通経路があり、その過程で模造品や不正機能を含む部品の混入等も想定される。そのため、製品のライフサイクルを想定したセキュリティ確認方法、認証制度を考慮されたい。特に、製造過程で模造品や不正機能を含む部品を検出する為の非侵襲攻撃技術（サイドチャネル攻撃など）を用いた不正機能検知技術開発の開発も検討する必要があると考えます。	製品のライフサイクルを踏まえたサイバーセキュリティ確保の研究開発を推進していく考えです。なお、不正機能検知技術の開発は本研究開発の対象範囲に含まれております。
7	1．P6の下から8行目 【意見】「～IoTシステムのセキュリティ・・・」とあるが、共通的に重要課題への対策としてGLが策定されるものと予想します。その際には各省庁毎ではなく共通対策ガイドとして頂きたい。 【理由】 IoT＆ビッグデータの時代では業界をまたがるサービスが種々存在する。セキュリティ対策を行う企業にとって各省庁毎の基準やGLを全て熟知するのは大変な負担である。従って、共通部分と業界個別部分に分けて策定すれば、対策を実施する企業にとっては業界ごとの特性を理解しやすく、また基準を策定する側にとっても各業種は個別部分のみを検討すればよいので、双方にとって相当な労力削減につながる。	ご意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
8	2.P8下から2行目 【意見】「・システムの運用時に、システムとして健全な状態であることを制御・通信機器および制御ネットワークの動作監視・解析から確認できる技術の実現」とあるが、これに加えさらに「解析結果から制御通信機器および制御ネットワークの攻撃防御設定を自動チューニングする技術の実現」を追加いただきたい。この自動チューニング技術によりIoTシステムにおけるサイバー攻撃耐性の飛躍的向上が見込める。 【理由】インシデント対応できるセキュリティ技術者は圧倒的に不足しているため、攻撃に応じて機器の防御設定を自動的に調整できれば迅速なサイバー攻撃対応が可能となる。	本計画案では、防御技術の自動化を含め、研究開発の公募対象としております。

9	3.P13（a3）制御・通信機器およびシステムの防御技術 【意見】「防御策については、重要インフラ分野ごとに判断基準が異なることから、・・・」とあるが、判断基準は共通部分も多くあり、防御技術はそのセキュリティ要件も含めて「分野共通部分」と「分野個別部分」とに分けて定義・開発していただきたい。 【理由】 国家的な見地において、セキュリティ技術者のリソースには限りがあるため、共通化できる対策はなるべく共通化するのがサイバーセキュリティ対策コスト低減の観点から有益である。	共通化は重要な考え方だと認識しております。可能な部分は極力共通化する方向で研究開発を進めるように致します。
10	・(2)研究開発項目(a4)で、「IoT向けセキュリティ確認技術」が掲げられているが、IoT機器が組み込まれるシステムでの役割により、さらされる脅威（不正機能を混入する目的やその機能）が異なるため、「IoT機器」の利用目的を明確にする必要があると考える。 ・「IoT機器上のソフトウェア」に対して「セキュリティ確認技術」とせず、「完全性・真正性を確認する技術」とした理由を明確にすべきである。	IoT機器の利用目的については、公募提案を踏まえて研究活動の中で利用目的を明確にしていきます。完全性・真正性の確認はセキュリティ確認の具体例です。
11	・認証制度を設計する前提となる、技術的要件、試験手順を含む試験要件の設定（設計）を行う過程（段階）を明示する必要がある。また、設定（設計）した技術要件、試験要件の妥当性・実施可能性を実証する過程（段階）を設ける必要があると考えます。 ・研究開発提案の採択基準ないし採択に関する考え方を予め公にしておく必要があると考えます。	認証制度の設計については、ご指摘の通りと考えます。具体的な設定や仮定などは、提案者として最適と考えられる提案をしていただくことを期待しています。採択基準や考え方については、後に準備される公募等書類をご参照ください
12	コア技術(a2)の制御・通信機器および制御ネットワークの動作監視・解析技術の開発においては、計画されていることも重要であるが、同時に、動作監視・解析におけるセキュリティ、すなわち、ログ等から得られる個人情報等の流出防止も重要であり、その対策も含んだ技術開発が重要である。 プロトタイプの実証試験として大学のキャンパスネットワークや実験用ネットワークを考えることも重要である。	ログ情報の保護は重要な課題であると考えます。実証環境については目的に沿って検討を進めるように致します。
13	セキュリティのコア技術は認証と暗号化でありその脆弱性は複製や成りすましの可能性と暗号基盤の擬似乱数にある。当社は原子核自然崩壊による真正乱数認証素子を開発し、NEDOのSTS助成事業で0.5mm角のチップとする計画である。量子事象による認証素子は人間が関与できず、兆の桁のエントロピーがある。この複製不能の物理基盤ですべてのインフラ機器を不正機能の混入やなりすまし不能な完全暗号通信機器にできる。	ご意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。
14	重要インフラである通信事業者の電気通信設備（昨今普及が進むVoIP、VoLTE等のIP電話システム）はオープンな外部ネットワークや制御ネットワークに接続されていることから、同設備のサイバー攻撃からの保護を本研究の対象とすべきと考えます。同設備のログ収集・分析からサイバー攻撃を検知・特定・防御することは一般的に難しく、ネットワークトラヒックからいち早く異常を検知・特定する技術の確立が必要と考え	ご意見の内容につきましては、今後の取組の検討に当たっての参考とさせていただきます。なお通信サービスは重要インフラの1つであり、本計画案の対象に含まれております。
15	研究開発計画（案）の8ページにあるように耐タンパーモジュールはセキュリティ確保のために有効であり、特にIoTのように計算能力や消費電力の制約が厳しい機器では不可欠である。他方、現在の耐タンパーモジュールには、バックドアの存在の指摘や、さらなる高度な暗号への対応等の課題が残されている。このため、耐タンパーモジュールの高機能化のための技術開発や、認証制度の高度化についても研究開発計画に含めることが必要。	耐タンパーモジュールの活用の重要性については、ご指摘の通りと考えております。具体的な研究開発の対象については、システム全体のセキュリティレベル底上げという観点から、公募の内容を踏まえ、優先順位付けを判断したいと考えております。
16	例えば、P9の21行目の「2．（1）①セキュリティ対策技術についてのシステムの要件」の「システム」など、本計画案の「2．研究開発の内容」の中には「システム」の文言が散見されますが、この「システム」が情報システムを指すのか、社会システムを指すのかが明確ではないため、その内容を明確に示す用語に修正する必要があると考えます。	システムは制御ネットワークを意味しています。2．（1）①の冒頭に次の説明を追記致します。 「本研究の対象は重要インフラの制御ネットワークであり、システムとはこれを実現する設備とその振る舞いを指す。」
17	P12下から5行目及びP13下から8行目にある「信頼の基点」について、その内容が明確ではないため、適切な用語に修正するか、用語の解説を加える必要があると考えます。	以下の用語解説を追記致します。 『信頼の基点とは（インターネット等で行われる電子的な証明が連鎖した構造を持つ認証基盤で用いられる概念「トラストアンカー」に類似する）、制御・通信機器のセキュリティを確認する手続きのために置かれる基点である。ここでいう制御・通信機器のセキュリティを確認する手続きとは、アクセスしている通信機器や動作させているソフトウェア等が正しいこと（真正性）を確かめたり、そのソフトウェア等が途中で改竄されていないこ と（完全性）を確かめることを意味する。』
18	例えば、P14末尾からP15冒頭にある「技術の有効性をプロトタイプ実装によって評価する」の「評価」など、本計画案の「2．（3）研究開発目標」の中には「評価」の文言が散見されますが、事業としての評価を行うのか、あるいは試行的な評価を行うのか、さらには、それら評価をどの機関が行うのかが明確ではないため、目標達成に向けた関係機関の役割等が不明確です。これらの点につき、明確にする必要があると考えます。	「2．（3）研究開発目標」では、「技術の有効性を評価する」としております。

19	P23の13行目～14行目の記述について、想定される社会実装先には、既存情報共有組織や既存認証組織などが含まれることから、「社会実装先として想定される各重要インフラ分野の所管省庁、既存情報共有組織、既存認証組織、民間事業者等の知見や技術を有効活用可能な研究開発体制を構築する。」と修正する必要があると考えます。	ご指摘を踏まえ、以下のとおり修文しました。 「社会実装先として想定される各重要インフラ分野の所管省庁、情報共有分析組織、認証組織、民間事業者等の知見や技術を有効活用可能な研究開発体制を構築する。」
20	本計画案は国際標準化活動をその出口として掲げていますが、P23の20行目の「利用される分野に応じ、標準化・規格化・安全評価手法やその認定手法の策定を推進し、開発成果の利用を促進」にある「認定」は、国際標準であるISO/IEC17000（適合性評価－用語及び一般原則）に定義されている「認定」とは意味合いが異なると思われるため、「確認」などの適切な用語に差し替える必要があると考えます。	ご指摘を踏まえ、p.23 20行目の「認定手法」を「製品認証手法」に修正致します。