

経緯

【 第24回情報セキュリティ政策会議（2010年7月22日）】

- 「情報セキュリティ2010」を政策会議において決定



- 「情報セキュリティ研究開発戦略(案)」を作成し、意見募集を実施

意見募集及び結果の概要

- 実施方法 : 内閣官房情報セキュリティセンターのWebページ上に掲載して公募
- 実施期間 : 2011年6月1日(水) ~ 10日(金)
- コメント総数 : 39件【内訳 : 9団体から延べ23件、4個人から延べ16件】
- コメント概要 : 施策に対する見解、施策実施に当たっての配慮要望等
 - ・ APT(Advanced Persistent Threats)に関する定義を明確にすべき。
 - ・ 攻撃者の行動分析による予防基盤技術に関し、誤解を与える表現は避け、十分に説明すべき。

コメントへの対応

- APTに関して修文を行い、脚注を追加した。
- 攻撃者の行動分析による予防基盤技術に関し、さらに詳細に説明した。
- いただいたご意見は、今後の政策運営にあたっての参考とするなど、適切に活用させていただく。

受付番号	枝番号	提出者	該当箇所	概要	ご意見に対する考え方
1	1	個人	5ページ 3-(1)-② 情報セキュリティの脅威の高度化・多様化(APTに関する記述)	APTは「概念」や「様態」であり、「手法」ではない。誤解を避けるために、「新しいタイプの攻撃」方法が生まれたわけではなく、すでに確立されている技術と人間系の手法を組み合わせ「攻撃という概念」の変化ととらえるべきである。	ご指摘を踏まえ、文章の表現を修正しました。また、APTの説明を注釈として追加しました。
2	2		12ページ 4-(2)-② 攻撃者の行動分析に基づくゼロデイ・ディフェンス(先読みの防御)	対象とする脅威が個人やコミュニティレベルならばよいが、より大きな組織レベルの攻撃に対しては、僅かの不確定要素で一気に防御を崩される危険もある。単に「技術研究」という枠組みでできるテーマではなく、また長期的にも実用化は難しいだろう。	ご指摘の内容については、今後の施策の推進の際の参考とさせていただきます。
3	3		13ページ 4-(2)-③ 個人情報等の柔軟管理の実現	こうした内容はすべてのリスク管理に共通であり、個人情報に限定することの弊害は大きいと考える。個人情報に限定されるべきではなく、リスク管理の柔軟化とすべきである。	当該部分は、重要分野を記載したものであり、推進すべき研究開発の内容を限定するものではありません。
4	4		21ページ 5-(3)-⑨ ITリスクに関する理論から実務までの体系化	最大の問題は、リスクの理解や対策、受容などの判断において、共通の尺度がないことであろう。ITの活用はそれが目的ではなく、こうしたアプローチを側面から支えていくというもの(手段)である必要がある。この部分はもっと強調されるべきである。	ご指摘の内容については、今後の施策の推進の際の参考とさせていただきます。
5	5		全般	情報セキュリティ戦略は、脅威と対象をある程度分類して、個々に課題を挙げていくべきなのではないか。	本文書は、今後、特に重要となる分野を重点化することを主眼としています。
6	6		全般	「研究戦略」は単体ではなりたない。今の日本の情報セキュリティの最も大きな問題は、人的・組織的な部分と技術分野が大きく乖離していることだと思う。前者をきちんと科学的に体系化し、その上で、それにどう「研究」「技術」を活かしていくかという全体的な視点が必要である。	本戦略は、我が国の情報セキュリティ政策の基本戦略である「国民を守る情報セキュリティ戦略(平成22年5月11日決定)」に基づき策定されるものであり、別途検討中の「情報セキュリティ普及・啓発プログラム」、「情報セキュリティ人材育成プログラム」等と併せ、情報セキュリティ政策全体を構成する一要素として位置付けられています。
7	1	札幌市医師会北区支部	全般	安全性確保と既存の有害事象及び今後起こり得る複数のリスクを定期的に再検証し、対策については国民や関係団体の同意を求めるよう要請する。	ご指摘の内容については、今後の施策の推進の際の参考とさせていただきます。
8	2		全般	あらゆる災害にも情報が失わることのないシステム構築し、個人情報を過剰な指導・監査や診療報酬削減の手段とする事がないよう要望する。	ご指摘の内容については、今後の施策の推進の際の参考とさせていただきます。
9	1	電子的本人認証の検討会	6ページ 3-(1)-③ 東日本大震災の発生	災害時に可用性を保持できる本人認証基盤を構築しておくことが必要である。自伝的記憶に基づく画像活用方式による汎国民的な本人認証基盤構築に向けた研究開発を加速させることを進言する。	ご指摘の内容については、今後の施策の推進の際の参考とさせていただきます。

受付番号	枝番号	提出者	該当箇所	概要	ご意見に対する考え方
10	1	日本ユニシス株式会社	9ページ 4-(1) 基本的考え方	ISO27000ベースの規程や各省庁が制定しているセキュリティ基準やガイドラインには、テロ攻撃を想定した対策要件が記述されておらず、また民間企業にはその知見がありません。安全保障上の観点から、『テロを想定した物理的セキュリティおよびシステムのセキュリティの研究』を追加すべきと考えます。	今後の施策の推進の際の参考とさせていただきます。
11	2		9ページ 4-(1) 基本的考え方	国内には、セキュリティに関する基準やガイドラインが多数存在し、システムを構築し運用する企業が混乱することがよくあります。企業が網羅的に参照できる『国内で統一されたセキュリティ基準・ガイドラインの策定』を戦略に追加してはいかがでしょうか？	本文書は、研究開発を対象としているので、ご指摘の内容については、情報セキュリティ政策全体の推進の際の参考とさせていただきます。
12	3		9ページ 4-(1) 基本的考え方	ネットワークを経由した取引の安全・安心の提供と、公共の福祉の増進に寄与するため、利用者がそのリテラシの高低にかかわらず、いつでもどこでも、ストレスなく使いこなせる、『⑧利用者重視の安心・安全なネットワーク社会の実現』を追加してはいかがでしょうか？	ご指摘の内容については、コンセプトのうち「情報通信システム全体のニュー・ディペンダビリティの確保」に包含されていると考えます。
13	4		12ページ 4-(2) 研究開発戦略のコンセプト	「性善説」で設計された現行インターネット上のセキュリティ問題は、根本的に新しいネットワークアーキテクチャを採用する必要がある。戦略の基本的な考え方に示されている「革新的な取組に重点を置くこととした」(P9中段)に鑑み、研究開発のコンセプトに『⑤厳密な匿名性とトレーサビリティの両方を同時実現するネットワークアーキテクチャの実現』を追加してはいかがでしょうか？	ご指摘の内容については、コンセプトのうち「個人情報等の柔軟管理の実現」に包含されていると考えます。
14	5		17ページ 5-(1)-① 実世界とコンピュータ内のモデル世界が融合した次世代ネットワークにおける情報セキュリティ基盤技術	『日本スマートフォンセキュリティフォーラムなどのような大規模な研究フォーラム連携し、有益な情報入手することにより、早期にスマートフォン情報セキュリティ基盤の実現を目指す』を追記してはいかがでしょうか？	今後の施策の推進の際の参考とさせていただきます。
15	6		3ページ 2-(2) これまでの情報セキュリティ技術の開発モデル	③ 万が一事後が起こった場合でも、 ⇒③ 万が一事故が起こった場合でも、	ご指摘の点を踏まえ、修正しました。
16	7		4ページ 2-(2) これまでの情報セキュリティ技術の開発モデル	システム可能性や事業継続性などの ⇒システム可用性や事業継続性などの	ご指摘の点を踏まえ、修正しました。
17	8		5ページ 3-(1)-① 情報報通信技術の変化	① 情報報通信技術の変化 ⇒① 情報通信技術の変化	ご指摘の点を踏まえ、修正しました。
18	9		25ページ 図7 重要テーマの技術ロードマップ	フォレンジックス等を支援するための ⇒フォレンジック等を支援するための	ご指摘の点を踏まえ、修正しました。

受付番号	枝番号	提出者	該当箇所	概要	ご意見に対する考え方
19	1	個人	全般	今回の資料は技術中心であり、情報セキュリティを包括的に捕らえた研究開発戦略ではない。情報セキュリティ分野での研究開発戦略とならば、管理・運用等のマネジメントや人間の行動を含めた研究開発戦略でなければならない。情報セキュリティ分野に心理学や行動科学等の分野の知見を利用する「情報セキュリティ心理学」等の分野の研究も必要になる。	本戦略は、我が国の情報セキュリティ政策の基本戦略である「国民を守る情報セキュリティ戦略（平成22年5月11日決定）」に基づき策定されるものであり、別途検討中の「情報セキュリティ普及・啓発プログラム」、「情報セキュリティ人材育成プログラム」等と併せ、情報セキュリティ政策全体を構成する一要素として位置付けられています。
20	2		25ページ 6 東日本大震災を踏まえた重点分野	BCPを見直せば、今回のような大災害に対策できるとは思われない。単に「非常用電源設備の強化」を行ったり、SNSがあれば次回もそれらが有効とは言えない。また、SNSでの「なりすまし」に関する対策も必要。バックアップにおいても遠隔保管など、メインフレーム時代でも常識であった。日本では、大地震、津波、台風・集中豪雨、テロを含めた広範囲な対応が必要であろう。	今後の施策の推進の際の参考とさせていただきます。
21	3		26ページ 6-(2)「リスク・マネジメント」等	リスクマネジメントを考える場合、「想定外」を想定すべきでない。想定外を限りなくなくし、対応できないのであれば別の対応を行う、あるいは検討を行ったことを記録化し、定期的に見直しを行うことが必要で、それがリスクマネジメントであろう。	今後の施策の推進の際の参考とさせていただきます。
22	4		21ページ 5-(3)-⑨ ITリスクに関する理論から実務までの体系化	体系化とあるが、記述内容は殆どそれに触れていない。情報リスクは大災害時だけの問題ではなく、重要基盤への攻撃から企業におけるものまであり、それらを体系化、その分野の研究開発を行っていくことが大切である。また、大災害、大規模攻撃を想定するのなら、運用におけるリスクの可視化等を含めた包括的なリスクマネジメントの体系化が必要であろう。	今後の施策の推進の際の参考とさせていただきます。
23	5		19ページ 5-(2)-⑤ 攻撃者の行動分析(プロファイリング等)	攻撃者の行動分析(プロファイリング等)は可能だろうか？ 高度な技術を持った攻撃者は海外在住のことが多く、また、犯人の特定も最近の事例では逮捕されていない。・プロファイリングより、事案のデータベース化を行い、犯罪防止に繋げることが大切であろう。	今後の施策の推進の際の参考とさせていただきます。
24	6		22ページ 5-(4)-⑪ セキュリティ部品が正しく実装されていることを保証する品質評価認証技術	セキュリティ部品の品質評価は有効か？ 現在、多くの製品は海外(米国やイスラエル、韓国等の)製品である。既に、ISO15408が認証を行っているが、その手間(認証取得に時間を要する、仕様書が日本語のみ等)がかなり、弊害の方が大きくなる。	今後の施策の推進の際の参考とさせていただきます。
25	7		4ページ他 「情報の非対称性」	情報の非対称性があると言ったことで済ませてよいのか？ 研究開発や教育を行うことにより、情報の非対称性を克服する努力を行っている。どんなに立派な研究開発戦略を考えても、それを推進する研究者・開発者を考えないで行うのでは、単なる研究開発予算の浪費になる。	今後の施策の推進の際の参考とさせていただきます。
26	8		3ページ 2-(2) これまでの情報セキュリティ技術の開発モデル	③ 万が一事後が起こった場合でも、 ⇒③ 万が一事故が起こった場合でも、	ご指摘の点を踏まえ、修正しました。

受付番号	枝番号	提出者	該当箇所	概要	ご意見に対する考え方
27	1	一般社団法人日本自動認識システム協会	18ページ 5-(1)-④ 生体情報をコンピュータで管理するためのID管理と生体情報を統合するシステム設計技術について	オープンなID管理システムに適用するシステム設計として、1社単独の方式に依存することなく、長期間に渡って存続し発展させることができる汎用的でオープンな仕組みを研究開発し、これを採用すべきだと思います。	今後の施策の推進の際の参考とさせていただきます。
28	1	個人	25ページ 6-(1)-② 災害時の情報システム	バイオメトリック認証は、所有物なしに体の一部を用いて本人を確実に特定できる技術であり、災害時の情報システムにおける本人確認手段として採用を検討すべきだと思います。	今後の施策の推進の際の参考とさせていただきます。
29	1		全般	現時点では、情報の多くは紙文書として存在していることから、セキュリティ政策の中に、「紙による情報漏洩」防止を入れて検討すべきである。	今後の施策の推進の際の参考とさせていただきます。
30	2	社団法人日本画像情報マネジメント協会(JIIMA)	全般	セキュリティ対策の委託研究を実施した実績と知見のあるJIIMAを加えて、セキュリティ政策をご検討・ご提案されたい。	今後の施策の推進の際の参考とさせていただきます。
31	3		全般	具体的には、電子情報だけではなく、紙文書の消失を防ぐ方法論も論じるべきである。情報管理者、情報管理規定、e-文書法の要件にしたがった電子化による一元管理で、今回の戦略案はその効果を増大することになる。	今後の施策の推進の際の参考とさせていただきます。
32	1	財団法人日本データ通信協会タイムビジネス協議会	21ページ 5-(3)-⑧ フォレンジック等を支援するためのデータ管理・追跡技術等	誰もが将来に亘って利活用できるべく標準ルールとして設定することが求められるため、ネットワーク上の信頼における時刻を活用することで情報の真实性を担保してその発生時点から収集・保存・管理・継承・解析を効率的に行うための技術研究とルールづくりが重要であると考えます。	今後の施策の推進の際の参考とさせていただきます。
33	2		25ページ 6 東日本大震災を踏まえた重点分野	紙文書保存から電子文書保存への移行が進んでいない実態を踏まえ、文書の電子保存を妨げている要因の分析と、その要因の一つとしてあげられるであろう「真正性と非改ざん性」を確保した運用方法の確立を研究開発戦略に追加すべきだと思います。	今後の施策の推進の際の参考とさせていただきます。
34	1		9ページ 4 情報セキュリティ研究開発戦略	情報セキュリティ研究開発は、技術、脅威の進歩に応じて見直しをしながら戦略を動的に見直すことが重要と考えます。ただし、方針を変更、調整を行う場合には、その理由を透明性をもって官民、さらに国際的な連携を十分の取ることが望ましいと考えます。	今後の施策の推進の際の参考とさせていただきます。
35	2	インテル株式会社	9ページ 4 情報セキュリティ研究開発戦略	情報セキュリティ研究開発は、社会で活用されることを目的とし、実利用に至るまでのロードマップを適切に描くこと、また定期的な見直しと道筋の再確認、課題解決が重要と考えます。具体的には研究、開発、実用化の間のギャップを見極めそれを埋めていく方法と手段を明確にしていくことが求められると考えます。	今後の施策の推進の際の参考とさせていただきます。
36	3		9ページ 4 情報セキュリティ研究開発戦略	パブコメは、30日の公開期間と、国際化の観点から英語版の文章による対応をお願いしたいと思います。	今後の情報セキュリティ政策の検討の際に参考とさせていただきます。

受付番号	枝番号	提出者	該当箇所	概要	ご意見に対する考え方
37	1	然株式会社	6ページ 3-(1)-③ 東日本大震災の発生	緊急時に自分しか知らない記憶をベースとした、自分を証明できる国家的な救済システムが必要である。	今後の施策の推進の際の参考とさせていただきます。
38	1	ネットワンシステムズ株式会社	20ページ 5-(2)-⑤ 攻撃者の行動分析による予防基盤技術	該当箇所の「脅威を洗い出し、対策の最適化」という言葉は、脅威が起こる可能性全てに、際限なく対策に備えるのかという印象を読者に与える恐れがあるので、「可能性」と「公算」の言葉を追加すべきであると考えます。 (修正案) 修正前:)行動予測モデルから脅威を洗い出し対策の最適化を行う、…。 修正後:)行動予測モデルから脅威の可能性を洗い出し、攻撃の公算を行った上で対策を検討することができる、。	ご指摘を踏まえ、該当部分を「攻撃の公算や影響を予測し」に修正しました。
39	1	個人	20ページ 5-(3)-⑦ 個人情報等の利活用を促進する自己情報の統制技術	医療情報に関しては、すでに厚生労働省、経済産業省、総務省からガイドラインが制定されている。それらのガイドラインと整合性を取って進めて頂きたい。	今後の施策の推進の際の参考とさせていただきます。