資料７

情報セキュリティ対策に関する官民連携の在り方について

平成２４年１月１９日

情報セキュリティ対策推進会議

官民連携の強化のための分科会

はじめに

政府は、防衛産業等への標的型攻撃の顕在化を踏まえ、官民における対策の強化について、情報セキュリティ対策推進会議（議長：竹歳誠内閣官房副長官。以下「CISO(Chief Information Security Officer)等連絡会議」という。）に「官民連携の強化のための分科会」を設置し、検討を行ってきた。今般、政府が講ずるべき情報共有等に関する対策を取りまとめたので報告する。

Ⅰ．標的型攻撃に対して政府が講ずるべき情報共有等に関する対策

標的型攻撃は、特定の組織を標的にして執ように攻撃を敢行し、その組織の特性、運用するネットワーク技術の特性に適合した高度で多様な手段を用いて、組織内の情報の窃取、組織の業務妨害等の目的で行われる。また、目標に到達するため、複数の目標への攻撃を連携させることで攻撃の効果を高めることも試みられる。

従って、標的型攻撃に対処するためには、個々の組織において攻撃を速やかに察知して適切な初動対処を実施するとともに、関連する組織間において脅威の情報を共有して集団的な対策を講ずることが望ましい。高度な技術を用いて長期間に執ように攻撃を行う主体は、攻撃に当たり相応のコストを払っていることから、そのコストに見合う攻撃対象が選定される。すなわち、国や国の防衛等に関する情報を扱う企業が高度な脅威にさらされている。そのため、官民が連携を強化することが標的型攻撃に対する有効な手段であると考えられる。

官民の連携に当たっては、漠然と組織間で情報共有を行うのではなく、各組織が情報セキュリティインシデントに関する緊急時対応の機能を有した専門的な部隊(以下「CSIRT(Computer Security Incidents Response Team)等」という。)を組織し、官民を含む各組織内 CSIRT 等の間で、専門的、実務的な連携を図ることが必要である。

以上、当分科会は、官民における CSIRT 等 の整備と各 CSIRT 等の間での情報連携の推進のため、以下の5分野について新たに9項目の対策を取りまとめた。

○5分野

（ｉ）政府としてとるべき方策、特に調達等に際して調達先企業に求める情報セキュリティ要件

（ii）政府と企業等との連絡・連携の在り方

（iii）産業界の取組に対する政府の協力、情報提供の在り方

（iv）企業等におけるセキュリティ文化の啓発、セキュリティ企業体質の涵養等

（ｖ）その他

(i)「政府としてとるべき方策、特に調達等に際して調達先企業に求める情報セキュリティ要件」について

●一般の調達等において、国の安全に関する重要な情報を扱う契約を締結する際には、情報セキュリティ上必要な事項を遵守するよう求める。

既に、情報処理に係る業務を府省庁の外部の事業者に委託する際には、「政府機関の情報セキュリティ対策のための統一管理基準」において、「委託先に請け負わせる業務における情報セキュリティ対策、機密保持、情報セキュリティの侵害発生時の対処方法、情報セキュリティ対策の履行状況の確認方法及び情報セキュリティ対策の履行が不十分である場合の対処方法を含む外部委託に伴う契約を取り交わすこと」、また、必要に応じて、情報セキュリティ監査の受入れ等を当該契約に含めることを定めている。また、「委託先における情報セキュリティ対策の遵守方法及び管理体制に関する確認書等を提出させること」も併せて定めており、さらに、再委託に際しては、再委託先にも情報セキュリティが十分確保される措置を委託先に担保させている。

国の安全に関する重要な情報を扱う契約は、情報処理に係る業務の外部委託にとどまらないことから、一般の調達等に際しても情報セキュリティ対策を契約で担保することとした。

企業等に求める要件については、調達仕様書、契約書等で用いることができる標準的なひな形を定める(付録1)。

ひな形を適用する契約は、国の安全に関する重要な情報を国以外の者に扱わせる契約とし、各府省庁において判断するものとする。

なお、ここでいう「国の安全」とは、国家の構成要素である国土、国民及び統治体制が害されることなく平和で平穏な状態に保たれていること、すなわち、国としての基本的な秩序が平穏に維持されている状態をいう。

ひな形には、(1)組織内 CSIRT 等を整備すること、(2)経営の責任者の関与と責任を明確にすることを企業等に求める事項として盛り込む。

また、調達契約を結んでいない、あるいは調達契約の及ばない「国の安全に関する重要な情報を扱う企業等」に対して同様な取組を促す方策を引き続き検討する。

(ii)「政府と企業等との連絡・連携の在り方」について

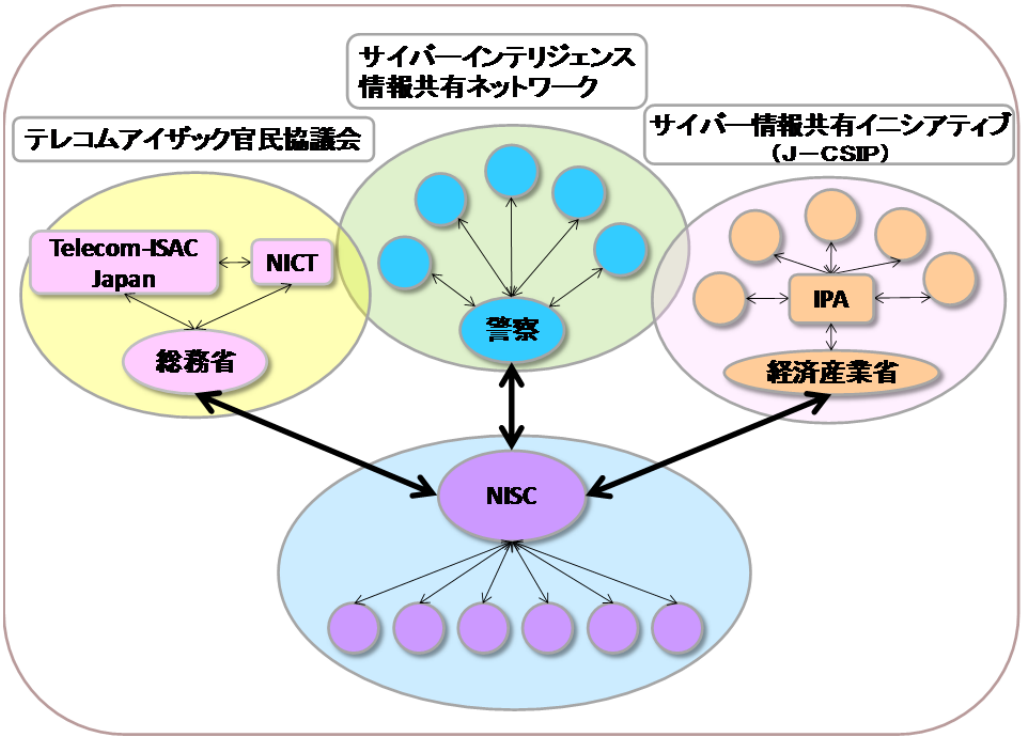
●CSIRT の横断組織である日本シーサート協議会や JPCERT コーディネーションセンター、情報セキュリティ事業者（SOC(Security Operation Center)事業者）、(独)情報処理推進機構と政府の調整役 CSIRT である内閣官房情報セキュリティセンターとの連携、情報交換の緊密化を図る。

緊急時に異なる機関同士が円滑に連携するためには、日頃から直接対面して各担当者間の人間関係を構築することが必要である。定期的な会合で意見交換を行うばかりでなく、日頃から技術的な相談を行ったり、共同で作業を行ったりするような機会を積極的に設けることも必要である。

そのため、CSIRT、 SOC 事業者、(独)情報処理推進機構(以下「IPA」という。)及び政府機関の担当者間でのインシデント対応のための連絡訓練や研修等を JPCERT コーディネーションセンター(以下「JPCERT/CC」という。)とも連携し、内閣官房情報セキュリティセンター(以下「NISC」という。)の主催で定期的に実施することを検討する。

●NISC は、警察庁のサイバーインテリジェンス情報共有ネットワーク、経済産業省のサイバー情報共有イニシアティブ(J-CSIP)、総務省のテレコムアイザック官民協議会等と NISC が運用する府省庁間のインシデント情報共有ネットワークとの情報連携の結節点の役割を果たす。

警察庁、経済産業省及び総務省は、それぞれのネットワークの情報のうち、可能なものは NISC 及び国内 CSIRT 等と共有することについて、それぞれのネットワークの参加者の了解を得た上で情報共有を図る。NISC は、政府機関で共有している情報のうち、サイバーインテリジェンス情報共有ネットワーク、サイバー情報共有イニシアティブ（J-CSIP）及びテレコムアイザック官民協議会と共有することが適切と判断するものについて、提供元の政府機関の了解を得た上で情報共有を図る。



(iii)「産業界の取組に対する政府の協力、情報提供の在り方」について

●SOC 事業者において、高度な対応を可能とするため、顧客の情報の一部を連携する諸機関と共有できるような標準的な契約、ひな形約款の策定に向けた検討を行う。

SOC 事業者は、契約に基づき顧客のネットワークを監視し、不審な通信、不審なシステムの挙動等のインシデントを検知して、顧客にインシデントの通報を行ったり、顧客のインシデント対応を支援したり、自ら顧客のインシデント対応を実施することをその業務としている。そのため、顧客の内部情報に接する機会も多く、通常は契約の中に秘密保持条項を定めたり、秘密保持特約を締結したりして業務に当たっている。しかしながら、各 SOC 事業者の秘密保持に関する規定はまちまちであり、SOC 事業者間での情報共有への取組も一様ではない。

SOC 事業者間で迅速に脅威に関する情報を共有することは、SOC 事業者全体の対処能力を向上させ、ひいては社会全体の情報セキュリティ水準の向上に資するものと期待される。このため、適切な情報共有が行えるような標準的な契約、ひな形約款の秘密保持条項の策定に向けた検討を行い、各 SOC 事業者間、及び SOC 事業者と NISC との間での情報共有の促進を図る。

(iv)「企業等におけるセキュリティ文化の啓発、セキュリティ企業体質の涵養等」について

●企業等における組織内 CSIRT 等の整備、情報セキュリティ人材の育成、標的型攻撃等の最近の情報セキュリティに関する状況等について広く官民で意見交換を行うためのシンポジウム等を開催する。

組織内 CSIRT 等は、まだ普及しているとは言い難く、CSIRT 等を担う人材も十分ではない。CSIRT 等の要員に求められる能力及び技能を客観的に評価するために、国家資格等を活用していくことなど、組織内 CSIRT 等の立ち上げを支援するための人材育成に係る普及・啓発を行う。

とりわけ、組織の情報セキュリティ対策については、CSIRT 等の要員など情報セキュリティ技術の専門家の育成と併せて、経営幹部や一般の従業員も含めたマネジメントスキルの涵養が重要である。すなわち、日常業務における情報、情報機器の取扱い、不審メールの受信等のインシデントに接した際の報告、連絡等の最初期の動作などについて広く啓発を行うことが必要であり、普及・啓発活動の一環として、多くの企業関係者等を対象としたシンポジウム等を平成23年度の情報セキュリティ月間中（平成24年2月）に開催する。

(v) その他

●我が国の政府機関（行政府のみならず立法府、司法府も含む。）においては、インシデントに機動的に対応するため、組織内 CSIRT 等を整備するなどして、標的型攻撃等に関する対策を遺漏なく継続的に実施する。

●NISC が政府機関の CSIRT 等間の連携・調整を行う政府の調整役 CSIRT となることを明確にし、標的型攻撃に関する対策も踏まえて政府統一基準群を改訂する。

各府省庁の特性に応じて、整備される CSIRT 等の様態も一様とはならないが、(1)「組織内向けにインシデント対応の窓口の明確化・一元化」、(2)「インシデントが発生している情報システムの稼働・停止等の実施又は勧告」、(3)「PoC (Point of Contact) の任命」、(4)「情報システムの理解、情報システム部門との相互連携」、(5)「NISC への報告」を「府省庁 CSIRT 等の必要5条件」とする。

現在も、行政府以外の立法府、司法府等にも CISO 等連絡会議のオブザーバとして NISC から情報提供を行っているが、CSIRT 等の整備等でも積極的に協力を行っていく。

CSIRT 等の整備や標的型攻撃への対策等について、次回の政府機関統一基準群の改訂の際に遺漏なく取り入れていく。

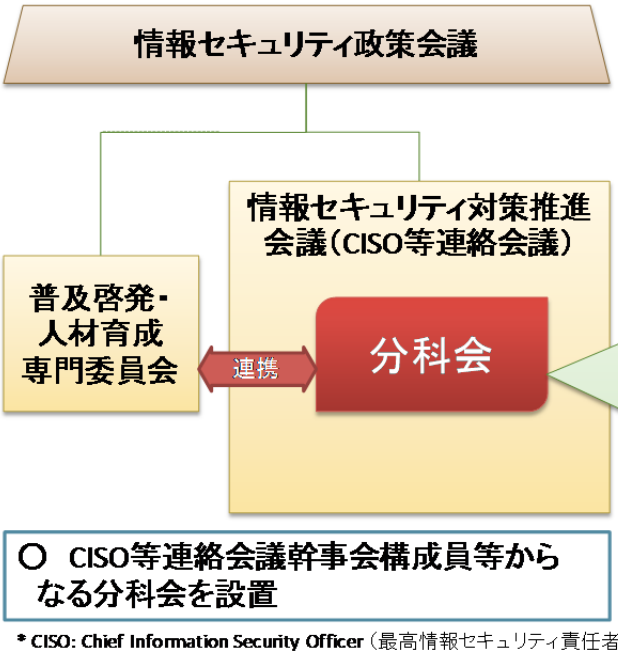
●政府として一元的に脅威に対処するため政府 CISO を新たに設置し、NISC センター長をもって充てる。

●CSIRT 等の要員の確保が困難な府省庁や、大規模なインシデント等により政府として迅速かつ的確に対応すべき事態が発生した際には、他の府省庁の CSIRT 等の要員による支援が可能となるよう、府省庁間協力のルール作りと NISC の調整機能の整備を検討する。

各府省庁の有する情報システムは、各府省庁自身が責任を持って情報セキュリティ対策を実施するのが原則である。しかし、緊急時には、政府が一体となって対処するため、政府 CISO が迅速な判断を行う局面も考えられる。　また、この様な緊急時等には、インシデントが発生している府省庁に対し、能力を持った者が組織を超えて機動的に支援できるサイバーインシデント版の DMAT（Disaster Medical Assistant Team 災害急性期に活動できる機動性を持ったトレーニングを受けた医療チーム）が必要となると思われる。

官民連携の強化のための分科会の設置

参考



平成23年

10月　7日　情報セキュリティ政策会議において設置方針の決定

10月14日　CISO等連絡会議において分科会を設置

官民連携等を通じて企業等の情報セキュリティ対策を強化するため、以下検討を行う。

(i)　政府としてとるべき方策、特に政府調達などに際して調達先企業に求める情報セキュリティ要件

(ii)　政府と企業等との連絡・連携のあり方

(iii)　産業界の取り組みに対する政府の協力、情報提供のあり方

(iv)　企業等におけるセキュリティ文化の啓発、セキュリティ企業体質の涵養等

官民連携の強化のための分科会　構成員

分科会長	内閣審議官（情報セキュリティセンター　副センター長）
構成員	危機管理審議官
	内閣参事官（情報セキュリティセンター）
警察庁	生活安全局情報技術犯罪対策課長 警備局警備企画課長 情報通信局情報管理課長
総務省	大臣官房企画課長 情報流通行政局情報セキュリティ対策室長
経済産業省	大臣官房情報システム厚生課長 商務情報政策局情報経済課情報セキュリティ政策室長
防衛省	運用企画局情報通信・研究課情報保証室長 経理装備局装備政策課開発・調達企画室長

付録１

調達における情報セキュリティ要件の記載について（案）

各府省庁大臣官房長等　殿
（　別　記　）

内閣官房副長官

各府省庁においては、国の安全に関する重要な情報を国以外の者に扱わせることを内容とする売買、貸借、請負その他の契約を行う際には、契約方式（一般競争、指名競争、随意契約（秘密随契、少額随契を含む。））に関わらず、調達仕様書及びこれに基づき作成する契約書（以下「調達仕様書等」という。）において、下記を参考として、当該契約の履行に当たって必要な情報セキュリティ要件を記載すること。

記

【調達仕様書等に記載すべき情報セキュリティ要件】

○ 情報セキュリティを確保するための体制の整備

本調達に係る業務を行う事業者は、事業者組織全体のセキュリティを確保するとともに、発注者から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。

本体制には、経営者が関与し、経営者の責任の明確化を図ること。

本体制における実務担当者には、「情報処理の促進に関する法律」（昭和45年法律第90号）に基づき行われる情報処理技術者試験のうち、情報セキュリティに関する資格を有する者若しくは同等の知識及び技能を有することを自ら証明出来る者を含むこととし、当該者については、継続して新たな知識の補充を行うことに配慮すること。

○ 取り扱う府省庁の国の安全に関する重要な情報の秘密保持等

本調達に係る業務の実施のために*［各府省庁名を記載］*から提供する国の安全に関する重要な情報その他当該業務の実施において知り得た国の安全に関する重要な情報については、情報のライフサイクルの観点から管理方法を定め、その秘密を保持し、また当該業務の目的以外に利用しないこと。

○ 情報セキュリティが侵害された場合の対処

本調達に係る業務の遂行において、定期的に情報セキュリティ対策の履行状況を報告するとともに情報セキュリティが侵害され又はそのおそれがある場合には、直ちに発注者に報告すること。これに該当する場合には、以下の事象を含む。

・受注者に提供し、又は受注者によるアクセスを認める*［各府省庁名を記載］*の情報の外部への漏えい及び目的外利用
・受注者による*［各府省庁名を記載］*のその他の情報へのアクセス

また、被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、発注者の求めに応じて成果物と共に発注者に引き渡すこと。

○ 情報セキュリティ監査の実施

本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するために、発注者が情報セキュリティ監査の実施を必要と判断した場合は、発注者がその実施内容（監査内容、対象範囲、実施者等）を定めて、情報セキュリティ監査を行う（発注者が選定した事業者による監査を含む。）。

受注者は、あらかじめ情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「情報セキュリティ監査対応計画書」等により提示すること。

また、受注者は自ら実施した外部監査についても発注者へ報告すること。

情報セキュリティ監査の実施については、これらに記載した内容を上回る措置を講ずることを妨げるものではない。

なお、「国の安全」とは、国家の構成要素である国土、国民及び統治体制が害されることなく平和で平穏な状態に保たれていること、すなわち、国としての基本的な秩序が平穏に維持されている状態をいう。

※ 国の安全に関する重要な情報を国以外の者に扱わせることを内容とする補助事業等の場合であっても、本通知による取扱いに準じ、当該補助事業等の履行に当たって必要な情報セキュリティ要件を補助金等の交付の条件として記載し交付決定すること。

（ 別 記 ）

内閣総務官
内閣法制局総務主幹
人事院事務総局総括審議官
内閣府大臣官房長
宮内庁長官官房審議官
公正取引委員会事務総局官房総括審議官
警察庁長官官房長、警察庁情報通信局長
金融庁総務企画局総括審議官
消費者庁次長
総務省大臣官房長
法務省大臣官房長
外務省大臣官房長
財務省大臣官房長
文部科学省大臣官房長
厚生労働省大臣官房長
農林水産省大臣官房長
経済産業省大臣官房長
国土交通省大臣官房長、国土交通省総合政策局長
環境省大臣官房長
防衛省運用企画局長、防衛省経理装備局長