資料３

政府機関等の情報セキュリティ対策のための統一基準群の見直し（骨子）

資料３－１　政府機関等の情報セキュリティ対策のための統一基準群の見直しについて（骨子）

資料３－２　統一基準群改定の方向性について

政府機関等の情報セキュリティ対策のための統一基準群の見直しについて（骨子）

資料3－1

1. 将来像を見据えたサイバーセキュリティ対策の体系の進化

①境界監視に加えプログラムが動作する内部（端末等）での挙動の検知による未知の不正プログラムに係る被害の未然防止／拡大防止、②IT資産管理の自動化とそれによる脆弱性への迅速な対応、③データ保護により事案が発生した際にも被害を無効化する情報漏えい対策の導入を、今後政府機関等が目指すべき3本の柱とし、第1段階としてこれらの対策の導入を推奨。

2. 政府機関等のサービスの利用者の側に立った対策

政府機関等は、自らの情報システムのサイバーセキュリティ対策に加え、国民が安心して安全にウェブサイト等を通じた行政サービスを利用できるよう、“利用者側に立った追加的な対策”を講じる時期。全ウェブサイト及び電子メール通信の暗号化対応の義務化。

3. 政府機関等の自律的な能力向上への誘導（PDCA※サイクルの効果的運用）

一巡した府省庁監査の結果から得られた知見を統一基準群にフィードバック。自らの対策状況を評価し、より効果的な改善に繋げるべく、政府機関等の自律的なPDCAサイクルの更なる循環を促す。

※ PDCA:[Plan（計画）、Do（実行）、Check（評価）、Act（改善）]

4. 多様な業務形態への対応

多様な業務形態が存在する独立行政法人等に目を向け、これらを踏まえたサイバーセキュリティ対策を導入。どのような業務形態であっても、安全かつ円滑に情報システムを利用できるよう、安全対策等を整備。

（スケジュール）
5月頃にパブリックコメントを実施し、夏頃にサイバーセキュリティ戦略本部決定を予定。

資料３－２

統一基準群改定の方向性について

１．現状認識と改定の必要性

（１）攻撃動向と対策の現状

・最近のサイバー攻撃では、検知されにくい未知の不正プログラムやスクリプトが使用されたり、ソフトウェアの脆弱性情報の公開直後に攻撃が開始されるなど、攻撃の成功確率の向上を狙った巧妙化が進展。また、国家の関与が疑われる洗練された高度なサイバー攻撃も発生。

・従来の防御システムでは検知されにくいサイバー攻撃を仕掛けることは、今や常套手段であり、従来の定義ファイル型の不正プログラム対策ソフトウェアでは有効な防御が困難な状況にある。また、このような状況の下では、境界監視において不正な通信が検知され初めて不正プログラムが実行されたことを認知することもあり、従来技術のみでは後追い対応にならざるを得ない場合があることも否定できない。

・2017 年のトピックとして、世界的規模でのランサム（身代金）ウェアによる攻撃が挙げられる。従来は、機微な情報や重要な社会インフラ等を取り扱う組織にとっては、「標的型攻撃」に対する対策が重要視されてきた。この重要性は今後も変わらないが、「ばらまき型攻撃」であるランサムウェアは、個人ユーザにとっては比較的少額の金銭を狙う攻撃であっても、これら組織にとっては機能停止を引き起こす別次元の攻撃となり得る。今後は、ばらまき型攻撃についても高い水準の警戒を行う必要がある。

・脆弱性を狙った攻撃に対しては、修正プログラムの適用等の迅速な対応能力が問われる。特にゼロデイ攻撃では、資産の最新状況の把握に基づいた機敏な対応が求められる場合もあり、これまでの人手による対応や外部委託先のみに依存した取組では、迅速性に限界があると言わざるを得ない。

・社会全体としては、IoT 機器を踏み台にした攻撃も発生しており、こうした攻撃への対策が喫緊の課題となっている状況である。

・他方、技術の進展とともに、サイバー攻撃に対する新たな防御技術が生まれてきており、今後サイバーセキュリティ対策の体系を大きく進化できる可能性も生じてきている。

（２）インターネット利用形態の変化

・サイバー空間における情報の窃取や改ざん、またウェブサイトのなりすましといった脅威が増大する中、インターネット上の情報及びその発信者に対する信頼の確保が大きな課題となっている。

・こうした中、通信される情報の盗聴や改ざんを防止するため、インターネット上での暗号化通信の割合が増加しており、インターネットによって国民に情報を提供する政府機関等は、この趨勢に沿って、より安心かつ安全に情報を提供する努力が必要となってきている。

・一方で、暗号化通信においては、従前どおりの境界監視が困難となる場合がある。したがって、必要に応じて境界監視を有効に機能させる対策や、新しい手法により不正プログラムを検知し、動作させない対策の導入などにより、引き続き監視・検知機能の維持・向上の取組が求められる。

（３）府省庁監査からのフィードバック

・2015 年のサイバーセキュリティ基本法の施行以来、NISC は府省庁監査を実施し、2016 年度末で全府省庁の監査を一巡した。監査結果により蓄積した知見から、改定に資するべき事項を抽出し、各府省庁の情報セキュリティ対策の向上に反映させることができる状況となった。

（４）独立行政法人及び指定法人への対応

・現行の統一基準群が改定された 2016 年 8 月は、改正サイバーセキュリティ基本法の施行（同年 10 月）前であったため、サイバーセキュリティ戦略本部に指定法人における対策の基準を作成する事務が追加されていない状況であった。一方で、各組織においては統一基準群の改定に伴いポリシー改定作業を行う必要があることから、統一基準群の改定手続は速やかに行う必要があり、改正法の施行前に統一基準群の改定を行った経緯がある。

・このため、前回改定時においては、統一規範及びその細則である統一基準、さらには対策基準策定ガイドラインの直接の適用対象は府省庁との従来の体系を維持するとともに、指定法人については独立行政法人と併せ、運用指針において統一基準群に基づく対策を求める（読替方式）こととし、改正サイバーセキュリティ基本法施行後の統一基準群の改定において府省庁、独立行政法人及び指定法人の全体を直接の適用対象として改めて整理することとしていた。このため、今次改定において、所要の規定の整理を行う必要がある。

・この際、府省庁の主たる業務は行政事務であり業務形態は全体として概ね一様であることに対して、独立行政法人や指定法人に目を向けた場合、多様な業務形態が存在していることに留意する必要がある。

（５）オリンピック・パラリンピックへの備え

・2020 年に予定されるオリンピック・パラリンピック開催期間を、全政府機関等が今般改定する統一基準群に基づいた新しいポリシーの運用状態で迎えることが望まれる。このため、2018 年度初めに統一基準群を改定し、遅くとも 2019 年度の早い段階で全政府機関等がポリシー改定を終える必要がある。

２．改定のコンセプト

（１）将来像を見据えたサイバーセキュリティ対策の体系の進化

・新たな防御技術の導入、システムによる自動化等により、サイバーセキュリティ対策を新たなレベルに進化させることができる時期に来ていると認識。

①エンドポイント検知による未知の不正プログラムの被害の未然防止／拡大防止

・未知の不正プログラムに対しては、従来のシグネチャ型の既知の不正プログラム検知方式では対応できず、境界監視により不正通信を検知した際はインシデント発生後とならざるを得ない。近年の技術進歩により、不正プログラムが動作する内部（端末等のエンドポイント）での挙動を検出することにより、インシデントの発生の未然防止や被害拡大防止の機能が向上してきている。

・このような機能の導入は、「監視」機能の高度化との視点でとらえることもできる。

②ＩＴ資産管理の自動化とソフトウェアの脆弱性への迅速な対応

・情報システムが高度化・複雑化する中で、多様な脆弱性が発生し、脆弱性情報の公開直後にこれを突くような攻撃が後を絶たない。人手による脆弱性対応は運用が限界に近づきつつあり、脆弱性対応を含むＩＴ資産管理の自動化による対応が効果的。

・このような機能の導入は、継続的な「監査」機能と捉えることもできよう。

③フェールセキュアによる情報漏えい対策

・オンプレミス、クラウドといったシステムの利用形態を問わず、インシデントが発生し、情報が外部に漏えいしても、内容を解読させないことにより、情報漏えい時のダメージを無効化する「フェールセキュア」の考え方を導入することが効果的。

・今後、上記①～③をセットとした対策を進めていきたい考えており、この政府機関等が目指すべき情報セキュリティ対策の将来像を見据え、今回の統一基準群の改定においては、これら対策の導入を推奨し今後の方向性を示すこととしたい。

（２）政府機関等のサービスの利用者の側に立った更なる対策（国民が安心して利用できる環境の整備）

・政府機関等の情報システム自体はサイバーセキュリティ対策を講じていても、インターネット上の政府機関等の外の情報システムがサイバー攻撃を受けることにより、政府機関等のウェブサイト等の情報が通信経路の途中で盗聴・改ざんされることがあり得る。このようなサイバー攻撃については、当該情報システムの所有者が対策を講じることが原則である。しかし、国民が安心して政府機関等のウェブサイト等のサービスを利用できるようにするためには、政府機関等は自らの情報システムのサイバーセキュリティ対策を講じるだけではなく、利用者の側に立った追加的な対策も講じる時期に来ていると考えられ、所要の改定を行う。

（３）政府機関等の自律的な能力向上への誘導（PDCAサイクルの効果的運用）

・マネジメント面に目を転じれば、サイバーセキュリティ基本法に基づく府省庁監査が全府省庁に対して一巡したところ、監査結果から得られた知見を統一基準群にフィードバックすることとする。

・府省庁全体として、統一基準に準拠した府省庁対策基準が求める必要な水準を満たすようサイバーセキュリティに係る取組が実施されていたことが確認されたが、更なる向上のため、各機関は対策状況を評価して改善を行う自律的な取組を強化し、PDCA サイクルを適切に運用することにより自律的な改善スパイラルを実現していくことを促す。

（４）多様な業務形態への対応

・業務を行う人間の側面に関する社会的変化として、業務形態が多様化してきている。特に今次改定に際しては、独立行政法人等の多様な業務形態を踏まえたサイバーセキュリティ対策の検討が求められる。

・このため、情報システムの利用技術も進展する中、どのような業務形態であっても安全かつ円滑に情報システムを利用できるように、所要の規定を整備する。