2012 年 12 月 14 日

独立行政法人情報処理推進機構（IPA）

サイバーインシデントの報告に関する、欧州連合（EU）における規制の状況

本概要は、欧州ネットワーク情報セキュリティ庁（ENISA：European Network Information Security Agency）が発行する、“Cyber Incident Reporting in the EU – An overview of security articles in EU Legislation”の抄訳となります。内容の詳細につきましては、原文をご参照ください。（※本文中のリンク先は全て英文となります）

URL：http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu

情報漏洩やハッカーによる不正アクセスなどサイバーインシデントの多くは、検知されないか、検知されても当局に報告されず、引いては一般にも公表されない。インシデント情報の透明性と情報の少なさは、インシデントの社会全体への影響や根本的原因、潜在的な相互依存性などの把握を困難にしている。

EU 加盟国の多くでは、デジタル社会の根幹を担う通信ネットワークおよび通信サービスを中心に、インシデント報告フレームワークが存在している。全ての加盟国に存在する訳ではなく、内容やアプローチも各国で大きく異なっている。インシデントが国境を越えて影響を及ぼす可能性があること、また、通信事業者やISPは複数国でサービスを提供しているケースも多く、EU統一的な規制が望まれる。EUでは、欧州委員会（EC）を通じて統一的な規制について話し合いを進めて来た。以降に、現行の EU 規制における関連条項の概要と、統一的なEU規制への課題を纏める。

現行の EU 規制における関連条項

1． 枠組指令（Framework Directive） 条項13a

2009年のEU Telecom Reform Packageにより改正。条項13aは公共通信ネットワークおよび通信サービスのセキュリティと完全性に関する項目で、以下を定めている。

- 公共通信ネットワークおよび通信サービス提供者（以下、「プロバイダ」）は、セキュリティと完全性を確保するための適切な対策を行うこと
- プロバイダは、深刻なインシデントについて、当該国の所轄機関（以下、「当局」）に報告すること
- インシデントが他国にも影響を及ぼす場合など、必要に応じて当局はENISAおよび他国の当局に通知すること
- 当局は、ENISAとECに年1回インシデント報告書を提出すること

13aの導入にあたっては、EC、ENISA、および各国当局が協力し、統一的な「対策基準」と「報告手順」を纏めている。

2． 電子プライバシー指令（e-Privacy Directive） 条項4

2009年のEU Telecom Reform Packageにより改正。条項4は、個人情報漏洩時の、当局への報告および契約者への通知に関する項目で、以下を定めている。

- プロバイダは、サービスのセキュリティを確保するために、適切な技術的、組織的対策を行うこと
- プロバイダは、個人情報の漏洩が発生した場合、当局に報告すること

- プロバイダは、個人情報の漏洩が契約者のプライバシーに悪影響を及ぼすと思われる場合、影響を受ける契約者に通知すること
- 事件に係る事実関係、影響、是正策を含めた、個人情報漏洩事件のリストを作成すること

ENISAでは、2011年に条項4の導入にあたっての技術的推奨策(ドラフト)を発行している。

3. データ保護に関する規制等(Data Protection Regulation) 条項30、31 および 32

EUデータ保護指令を改正。条項30～32は、個人情報を扱う組織におけるセキュリティ対策と漏洩時の報告に関する項目で、以下を定めている。

- 個人情報を扱う全ての組織は、処理プロセスにおけるリスクに応じて、セキュリティを確保するため、適切な技術的、組織的対策を行うこと
- 全てのビジネス業界において、個人情報漏洩時の通知を義務付けるものとする(※対象を、通信ネットワーク業界から全業界に拡大)
- 個人情報の漏洩が発生した場合、遅延なく、可能であれば24時間以内に、当局に報告すること。遅れた場合、正当な理由があること
- 個人情報の漏洩が個人のプライバシーに影響を及ぼすと思われる場合、個人に通知すること。なお、情報が見れない状態になっている場合は、通知しなくてもよい(※前述のENISAのガイドラインでは、暗号化またはハッシュ化を推奨)

4. 電子署名および電子IDに関する規制(e-Sig and e-ID Regulation) 条項15

ECによる、電子IDおよびウェブサイトの認証やタイムスタンプなど、電子署名や証明書等の技術を利用して提供されるあらゆるサービス(以下、「トラストサービス」)に関する規制。条項15は、セキュリティ対策およびインシデント発生時の報告に関する項目で、以下を定めている。

- トラストサービスのプロバイダは、セキュリティを確保するため、適切な技術的、組織的対策を行うこと
- トラストサービスのプロバイダは、インシデントが発生した場合、当局および他の関係機関に報告すること。必要に応じて、当局は、他のEU加盟国の当局およびENISAに通知すること
- 当局は、直接、またはトラストサービスのプロバイダを通じ、一般にインシデントについて通知すること
- 当局は、インシデントの概要を、ENISAおよびECに送付すること

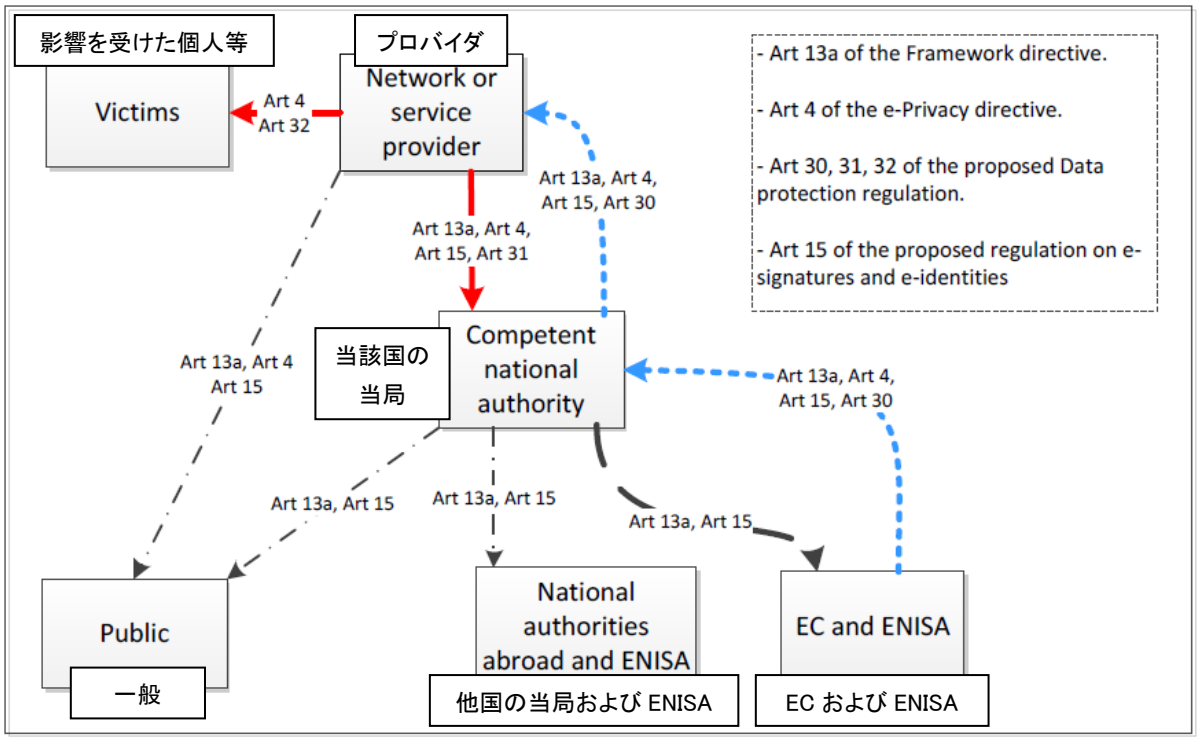
5. 欧州サイバーセキュリティ戦略(EU Cyber Security Strategy)

現在ECは、欧州におけるサイバーセキュリティ戦略の策定を進めており、ロードマップでは枠組指令の条項13aの対象を、通信ネットワークおよび通信サービス業界から、他業界に拡大することなどが示唆されている。大きくは、5つの課題が取り上げられると見られている。

- 官民情報共有機能とネットワークの確立
- インシデントについて検討し、EUとしての緊急時対応計画を策定するための体制の整備
- 電力、金融、輸送などの重要インフラ分野におけるインシデント報告の促進
- 欧州全体を1つの市場とし、セキュリティ技術を発展させるための、セキュリティ技術開発を促進する前衛的な調達戦略(pre-commercial procurement)と、官民パートナーシップの強化

- グローバルレベルでの相互依存性とサプライチェーンについて検討するための国際協力

現行の EU 規制における関連条項のモデル化（図中の番号は、本文中の条項を示す）



赤：通知・報告　**水色：対策技術（情報）の提供**　黒色（細）：通知　**黒色（太）：年次報告書の提出**

統一的な EU 規制への課題

以下に、EU全体としてインシデント報告や対策を検討するにあたっての、課題を幾つか記す。

- 規制の曖昧な個所のカバー

  現行の規制や検討中の欧州サイバーセキュリティ戦略では、報告の対象でない（対象かどうか明確でない）事例も存在する。規制を改正せずとも文言の解釈を明確にすることで対応できるところでもあり、明確化に向けての取組が必要とされる。

- 関連法規（条項）のモデル化

  枠組指令の条項13aと、欧州サイバーセキュリティ戦略の条項15は非常に類似している。整合性を持たせ、文言を標準化するなど整備すれば、より各国での導入がし易くなると思われる。

- セキュリティ対策の管理

  対策の目的は、個人情報の漏洩やインシデントの影響を軽減、できれば防止することだが、対策は技術的な実装に大きく依存するところであり、詳細をEU規制のレベルで規定することは非合理的である。当局は効果的・効率的な規制および技術的な要件が何か協力して検討することが望ましい。また、ボトムアップ・アプローチを取り、現場のベストプラクティスを生かせる形にするのが重要である。関連条項の中に頻出する「適切な技術的・組織的対策」については、企業、業界、国によらず共通点も多いと思われる。そうした対策については、当局が国レベル・EUレベルで協力し、コンプライアンスが容易になるよう取り組むべきである。

- インシデント報告プロセスの最適化

当局へのインシデント報告の義務付けは、企業が法規に従っているかを確認するためであり、インシデント情報の共有は、当局（国）もインシデント対応に取り組むためである。加盟国は、トランスペアレントで信頼できる情報共有環境を奨励すると共に、報告プロセスがインシデント対応の妨げとならないよう、簡単にすることが必要である。また、規制の評価を、費用と利益のバランスから考えることも重要である。報告が少ないと、分析しても意味のある情報は得られない。当局は、費用対効果に見合うバランスを見極めつつ導入することが大切となる。企業が必要十分な情報を簡単に報告できるよう、ツールの活用等も検討すると良い。

ENISAでは、来年以降、毎年春に各加盟国の当局から集まる報告を纏めて公開すると共に、各国の当局およびECと協力し、今後もEU規制の導入・改善を支援していく。

以上