サイバーセキュリティのための情報共有に関する米国と EU の法制比較

2016- 10- 12（第 1 版）、2017-5-15 （第 2 版）　林　紘一郎

項目	米国	EU
根拠法	2015 年サイバーセキュリティ情報共有法（2015 年サイバーセキュリティ法の一部）	The Directive on Security of Network and Information Systems (NIS Security Directive)
制定日	2015 年 12 月 18 日（両院協議会可決）	2016 年 5 月 17 日（EU 理事会で採択）、7 月 6 日（欧州議会で可決）
効力発生日	2015 年 12 月 18 日（大統領署名）	Directive なので、加盟国は 21 か月以内に国内法化し、27 か月以内に Operator of Essential Service (OES)等を指定する義務がある
目的	(1) 以下の懸念の払拭。① 民間が政府と共有したデータが情報開示される恐れ、② 共有データに含まれる個人データのプライバシー問題、③　独禁法違反の可能性、④ 提供情報により違法行為が指摘される危険。 (2) 事故情報（後述の CTI と DM）によるサイバー攻撃への対処策の向上	(1) 加盟国に以下の義務を課す。① NIS に関する国家戦略の策定、② 協調グループの設置、③ CSIRT ネットワークの構築、④ OES（上述）Digital Service Provider（DSP）に対するセキュリティ・レベルの確保と事故通知、⑤ 所管官庁（National Competent Authority = NCA、複数も可）、単一のコンタクト・ポイント（SPoC）、CSIRT の指定。 (2) 国家安全保障と重大犯罪捜査は別扱い
情報共有者	連邦政府と非政府機関（後者に、地方政府を含む）	中央政府と OES および DSP 間
情報共有の義務	義務はなく非政府機関の任意。また政府は調達などを通じて強要してはならない	OES および DSP として指定された者とっては義務。指定されない事業者にとっては任意
共有情報または情報提供者の定義	(1) 共有情報 ① 機密指定された CTI (Cyber Threat Information) と DM (Defensive Measures)、② 機密指定されていない CTI と DM、③ Best Practice (2) 用語の定義　CTI には、次の 8 つの態様を含む。	(共有情報の定義) リスク（NIS に悪影響を及ぼす可能性があると合理的に特定可能な環境またはイベント）に関する重大な情報 （情報提供者の定義）OES とは、(a) 社会に不可欠なサービスを提供し、(b) サービス提供が NIS に依存し、(c) 事故がサービス提供

	① 脆弱性情報の収集などの偵察、② 脆弱性の利用方法、③ 脆弱性を前提にした特異な行動、④ ユーザの合法的アクセスによりセキュリティ管理を破る方法、⑤ 悪意の C&C、⑥ 秘密裏に盗み出された情報など顕在・潜在の被害、⑦ 法によって禁じられていない、その他の特性、⑧ これらの組み合わせ。一方 DM とは、既知または疑わしい脅威または脆弱性を、探知・予防または軽減するために、情報システムまたは情報そのものに、保存・処理・送信された情報に適用される行為で、デバイス・手法・シグナチャー・技術・その他の方法をいう。ただし、他者の情報システムまたは情報そのものを破壊し、不正なアクセスを可能にしまたは重大な害悪を及ぼすものは含まない。	に壊滅的な影響を及ぼす事業者。DSP とは、デジタル・サービスを提供するすべての法人であるが、NIS においては「オンライン・マーケット、検索エンジン、クラウド・コンピューティング」の 3 種に限られている。
共有方法	(1) 非政府機関は次の情報をモニターできる、① 自己の情報システム、② 承諾を得た他者のシステム、③ 連邦行政機関のシステム、④ 民間によりモニターされたシステムに保存・処理・送信された情報。 (2) 非政府機関は CTI と DM を相互にまたは連邦政府と共有できる。	(1) OES はサービスの継続に深刻な影響がある事故を、遅滞なく所管官庁（NCA）に通知する義務がある。提供される情報は、機密性が保たれる。受け取った側はフォローアップ情報を提供しなければならない。単一のコンタクト・ポイント（SPoC）は、影響を受ける他の加盟国に送付する。個別の事故情報が事故の予防等に役立つ場合には、提供者と協議して公表できる。 (2) 加盟国は NCA に、OES に対して次の事項を要求できる権限を付与しなければならない。① セキュリティ・ポリシーの策定と提供、② セキュリティ監査結果などの証拠の提供。ただし、要求の目的を

		明記し、情報を特定しなければならない (3) DSP はサービス（オンライン・マーケット、検索エンジン、クラウド・コンピューティングに限る）の継続に深刻な影響がある事故を、遅滞なく所管官庁等に通知する義務がある。ただし、義務が発生するのは対象利用者・事故期間・地理的広がりなどを見積もり得る場合に限る。また提供される情報は、機密性が保たれる。なお、OES が依存する DSP の事故は、OES が通知しなければならない (4) 受領した所管官庁等は、影響を受ける他の加盟国に送付する。また個別の事故情報が事故の予防等に役立つ場合には、提供者と協議して公表するか、公表を求める。 (5) 加盟国は NCA に、DSP に対して次の事項を要求できる権限を付与しなければならない。① NIS セキュリティを検証するための情報の提供、② 必要なセキュリティ・レベルに達していない場合の改善。なお DSP が、加盟国に複数の施設が代表者を置いている場合は、主たる施設か代表者の加盟国が、他の加盟国と相互に協力する。 (6) DSP に関する規定は、小企業・零細企業には適用しない。
個人データの保護	① サイバー脅威に関連しない個人データの削除、② 個人データ漏えいの場合の本人への通知義務	GDPR（General Data Protection Regulation、Regulation (EU) 2016/679 に移行。2018 年 5 月以降適用。
主務官庁	DHS（国家安全保障省）。大統領は他の官庁を追加指定できる	加盟国ごとに指定(複数可だが、1 の場合には、同時に単一のコンタクト・ポイントにもなる)
連邦政府による利用と	(1) 保持又は利用できるケースを次の 5 つに限定。① サイバーセキュリティに関する目的、② 脅威または	

開示の制限	脆弱性の特定、③ テロ行為など具体的な危険の阻止・軽減、④ 未成年者の搾取などの危険の訴追・軽減、⑤ それから生ずる具体的な犯罪等の予防・軽減。(2) 共有情報の開示は禁止（FOIA = Freedom Of Information Act of 1966 の適用除外）	
独禁法上の免責	DOJ（司法省）と FTC（連邦取引委員会）の Anti-trust Policy on Sharing of Cybersecurity Information を追認	
民間企業の訴追からの免責	民間企業のモニタリング行為や情報共有は、訴訟原因とならない	
具体的手続	① 2015 年サイバーセキュリティ情報共有法における共有を支援するための指針（2016 年 2 月 16 日 DHS） ② 2015 年サイバーセキュリティ情報共有法における CTI と DM の共有（DNI、DHS、DOD、DOJ） ③ 連邦政府による CTI と DM の受領に関する暫定手続（DHS、DOJ） ④ プライバシーと人権支援に関する暫定手続（DHS、DOJ）	加盟国にはレベル差があるので、底上げする機能は ENISA（European Union Agency for Network and Information Security）が担うものと思われる。現に ENISA は、その覚悟があることを表明している（ENISA [2016] 'ENISA's Position on the NIS Directive'）。
自動 CTI 共有システム（Automated Indicator	2016 年 3 月 21 日、NCCIC（National Cybersecurity and Communications Information Center）で運用開始	

Sharing = AIS）		
裁判管轄と準拠法	アメリカ国内の裁判所とアメリカ国内法	DSP は主たる常備施設（あるいは本社）がある加盟国の裁判管轄に属する。域内に設立されていないが、域内でサービスを提供している DSP は、域内の代表者を指名し、その代表者が置かれた加盟国の裁判管轄に属する。代表者の辞任によって、訴訟を免れることはできない。
罰則	任意規定なので罰則はない	加盟国は効果的でバランスのとれた罰則を策定しなければならない

Briefing paper 等による「事業者の権利（あるいは免責）と義務等」に関する補足

<table>
<tr><th>項目</th><th>米国</th><th>EU</th></tr>
<tr><td>事業者の権利あるいは免責）と義務等</td><td>１．事業者の権利（免責）
・自己（あるいは委託された）情報システムに対して defensive measures を取ることが許される
・CISA の手順に従う限り免責が得られる
・免責は、民事裁判・業法による規制・独禁法違反と幅広い
・共有情報も指定すれば proprietary なものとして維持できる
・共有情報は情報公開法の適用除外になる
・情報共有中も、監督官庁との対話を継続できる
２．事業者の義務
・共有は任意であって、強制されない
・共有情報から個人特定情報を除かなければならない
・脅威情報等を受け取ったからといって、エンド・ユーザに警告</td><td>
<table>
<tr><th>義務</th><th>OES</th><th>DSP</th></tr>
<tr><td>リスクへの技術的・組織的対処</td><td>○</td><td>○（一部）</td></tr>
<tr><td>セキュリティ・ポリシー等の情報提供</td><td>○</td><td>○</td></tr>
<tr><td>監査など実効性の証拠の提供</td><td>○</td><td>×</td></tr>
<tr><td>NCA の命令等の実行</td><td>○</td><td>×</td></tr>
<tr><td>指令に反した場合の補償措置</td><td>×</td><td>○</td></tr>
<tr><td>常備設備を持たない場合の代表者の指名</td><td>×</td><td>○</td></tr>
</table>
</td></tr>
</table>

	したり利用者のために行動する直接の義務はない（通常の「善管注意義務」はある） ３．政府の義務 ・官民共有は DHS の所管（長年の権限争いを整理） ・政府の情報利用は法の定める目的に限定（特に EU との間では、Privacy Shield agreement による制約＝次表）	
出典	Sullivan and Cromwell [2015] 'The Cybersecurity Act of 2015', https://www.sullcrom.com/.../SC_Publication_The_Cybersecurity_A..	Deloitte [2015] 'Agreement reached on EU NIS Directive' https://www2.deloitte.com/lu/en/pages/risk/articles/agreement-new-eu-network-information-security-directive.html

-

EU Privacy Shield による取得情報の利用制限に関する補足

	US-EU Privacy Shield による制限
取得情報の利用制限	・2015 年 10 月の EU 司法裁判所による Safe Harbor agreement 無効判決を受けたもの。2016 年 7 月発効。 ・米国企業は商務省が定める Privacy Shield の条件をクリアすれば、EU データ保護指令が定める adequate level of protection に達していると認定 ・政府による EU 市民データへのアクセス制限。特に、バルク・データの取得と利用を、国家安全保障に関する場合のみ例外とするとともに、国務省にオンブズマンを置き侵害から救済 ・救済手段として、ADR（Alternative Dispute Resolution）、米国 FTC との連携による自国の Data Protection Agency への申し立て、仲裁措置、（国家安全保障に関してのみ）オンブズマンによる解決などを用意 ・USA と EU 共同による毎年の見直し
出典	EU Commission [2016] "European Commission launches EU-U.S. `Privacy Shield: stronger protection for transatlantic data flows' (Press Release)　http://europa.eu/rapid/press-release_IP-16-2461_en.htm