規則(EU) 2018/1862

［参考訳］

2019 年 5 月 17 日
明治大学法学部教授
夏 井 高 人

＊＊＊

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU（OJ L 312, 7.12.2018, p.56-106）のテキスト（英語版）に基づき、和訳を試みた。テキストは、下記の Eur-lex の Web サイトから入手した。

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1862&from=EN
[2019 年 5 月 9 日確認]

規則(EU) 2018/1862 は、警察分野及び法務分野におけるシェンゲン情報システム（SIS）の利用に関する EU の基本法令の 1 つである。規則(EU) 2018/1862 により、従前の幾つかの関連法令が統合され、廃止された。

EU の対外国境警備の分野におけるシェンゲン情報システム（SIS）の利用に関する EU の基本法令は、規則(EU) 2018/1861（OJ L 312, 7.12.2018, p.14-55）である。EU の対外国境における出入国管理のためのシェンゲン情報システム（SIS）の利用に伴う個人データの保護に関する EU の基本法令は、規則(EU) 2018/1860（OJ L 312, 7.12.2018, p. 1–13）である。

COM(2019) 3 final により、規則(EU) 2018/1862 を一部改正する提案が既に行われている。この改正提案は、規則(EU) 2018/1240（OJ L 236, 19.9.2018, p.1-71）により設置された ETIAS との相互運用性（interoperability）を確保するために、第 18 条 a を追加し、第 44 条第 1 項に(f)を追加し、第 50 条 a 及び第 50 条 b を追加するというものである。

規則(EU) 2018/1862 は、前文、条文及び別紙の 3 つの部分で構成されている。この参考訳においては、規則(EU) 2018/1862 の前文、条文及び別紙の全文を訳出した。

この参考訳においては、原則として直訳とした。直訳のままでは日本語として意味の通らない部分や非常にわかりにくい部分に関しては、やむを得ず意訳とした。

この参考訳は、あくまでも規則(EU) 2018/1862 の私的な和訳であり、関連分野の研究者のための参考として提供するものである。確定訳ではなく、現時点における検討結果の一部を示すものであるので、今後、必要に応じて改訂・修正が加えられる可能性がある。誤記等があるときは、随時、法と情報雑誌上においてその正誤を公表する。

この参考訳に訳注はない。脚注は、全て原注である。

規則(EU) 2018/1862 の前文は、全体として、規則(EU) 2018/1861 の前文と同一またはほとんど同じものであるが、規則(EU) 2018/1862 の前文(23)～(43)は、規則(EU) 2018/1862 に固有のものとなっている。規則(EU) 2018/1862 の前文(23)～(43)においては、捜査活動に伴う生体データの利用と関連する法的問題など、規則(EU) 2018/1862 の固有の目的と密接に関連する事項を示している。

規則(EU) 2018/1862 の前文(3)にある報告書とは、「Report from the Commission to the European Parliament and the Council on the implementation of the Regulation (EU) No 1025/2012 from 2013 to 2015」（COM(2016) 212 final）のことを指し、スタッフ作業文書とは、「Commission Staff Working Document: Analysis of the implementation of the Regulation (EU) No 1025/2012 from 2013 to 2015 and factsheets Accompanying the document Report from the Commission to the European Parliament and the Council on the implementation of the Regulation (EU) No 1025/2012 from 2013 to 2015」（SWD(2016) 126 final）のことを指す。

規則(EU) 2018/1862 は、実質的に見て、理事会枠組み決定 2002/584/JHA（OJ L 190, 18.7.2002, p.1-20）の一部改正法令として機能する部分を含んでいる。それゆえ、規則(EU) 2018/1862 全体を正確に理解するためには、理事会枠組み決定 2002/584/JHA の全文を同時に精読し、理解しなければならない。また、これら 2 つの法令の相互関係ないし論理関係の詳細に関しては、今後、更に検討を要する。

規則(EU) 2018/1862 に基づく個人データの送受信に関しては、規則(EU) 2018/1725（OJ L 295, 21.11.2018, p.39-98）及び指令(EU) 2016/680（OJ L 119, 4.5.2016, p.89-131）が適用される。その個人データの処理、特に監督機関による監督及び EDPS による監督に関しては、規則(EU) 2018/1725 及び指令(EU) 2016/680 の正確な理解を必須の前提としている。そのような正確な理解を前提とすることなく、抽象的に「犯罪捜査におけるプライバシー保護」を論じてみたとしても、基本的に無力である。

EU の機関及び組織に適用される個人データ保護のための基本法令であった規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1-22）は、規則(EU) 2018/1725 の第 99 条によって、2018 年 12 月 10 日の経過をもって廃止された。規則(EC) No 45/2001 に対する参照は、規則(EU) 2018/1725 への参照として読み替えられる。

規則(EU) 2018/1862 の第 60 条第 7 項と規則(EU) 2018/1861 の第 45 条第 7 項を比較すると、後者の原文の中に明らかな誤記が存在することを理解できる。

（この参考訳を作成するに際し考慮した事項）

「police cooperation and judicial cooperation」については、従前は、日本国の外務省の訳を尊重し、「警察共助及び司法共助」と訳してきた。しかし、これまでの検討結果を踏まえると、少なくとも EU 法に関する限り、「警察共助及び司法共助」との訳では「police cooperation and judicial cooperation」の機能・内容を正確に示すものではなく、かつ、本来の意味における共助（mutual assistance）との識別ができない

という問題がある。

そこで、この参考訳は、EU における実際の機能・内容に即し、「police cooperation and judicial cooperation」を「警察協力及び法務上の協力」と訳すことにした。

これと異なる従前の参考訳中の訳は、一括して改める。

EU の構成国間における欧州逮捕令状（European Arrest Warrant）による「surrender」、EU の構成国と第三国との間における国際条約・国際協定等に基づく「extradition」の訳語に関しては、後掲理事会枠組み決定 2002/584/JHA の参考訳の冒頭部分においても述べたとおり、様々な問題がある。特に、その両者が混在する文において、どちらの語も「引渡し」と訳すと、識別性が喪失してしまうという問題がある（規則(EU) 2018/1862 の前文(28)、前文(29)参照）。

この参考訳においては、後掲理事会枠組み決定 2002/584/JHA の参考訳において採用した方針を維持し、「surrender」を「身柄引渡し」と訳し、「extradition」を「引渡し」と訳すことにした。

「discreet checks」、「inquiry checks」及び「specific checks」は、いずれも、EU の対外国境における機械的かつ自動的な検問ではない検問のことを意味する。その内容の詳細に関しては、ETIAS 規則(EU) 2018/1240（OJ L 236, 19.9.2018, p.1-71）の前文の中に説明がある。

これらの語に関しては、後掲 ETIAS 規則(EU) 2018/1240 の参考訳における検討結果を踏まえ、それぞれ、「詳細な検問」、「質問による検問」及び「個別の検問」と訳すことにした。

「travel document」は、一般に、「渡航文書」または「渡航書」と訳されている。しかし、船舶及び航空機を一切使用しない陸路のみの移動の場合、「渡航」という語が不適切である。

以上を踏まえた上で、この参考訳においては、「travel document」を「旅行文書」と訳すことにした。

「suspects」及び「accused persons」は、日本国の刑事訴訟法においては「被疑者」及び「被告人」に相当するが、EU の構成国において法制上の相違が存在すること、それらの者に与えられる刑事手続上の権利も日本国の法制の下における権利とは異なるものであり得ることを考慮に入れると、単純に「被疑者」及び「被告人」と訳すと様々な問題が生ずるおそれがあることを否定できない。

そこで、この参考訳においては、「suspects」及び「accused persons」を「容疑者」及び「被訴追者」と訳すことにした。

規則(EU) 2018/1862 の第 37 条第 4 項の末尾を含め、単純な誤記と推定される箇所が散見されるが、適宜、合理的に解釈した上で翻訳することにした。

以上のほかは、後掲 eu-LISA 規則(EU) 2018/1726 の参考訳、後掲 ETIAS 規則(EU) 2018/1240 の参考訳、後掲規則(EU) 2018/1861 の参考訳、後掲規則(EU) 2018/1241 による改正後の Europol 規則(EU) 2016/794 の参考訳、後掲 Eurojust 規則(EU) 2018/1727 の参考訳、後掲規則(EU) 2018/1860 の参考訳、後掲理事会枠組み決定 2002/584/JHA の参考訳の各冒頭部分で述べたとおりである。

（訳出済みの関連法令等及び参考文献）

規則(EU) 2018/1241 による改正後の Europol 規則(EU) 2016/794 の参考訳は法と情報雑誌 4 巻 4 号 8～68 頁にある。Eurojust 規則(EU) 2018/1727 の参考訳は、法と情報雑誌 4 巻 5 号 1～60 頁にある。

eu-LISA 規則(EU) 2018/1726 の参考訳は、法と情報雑誌 4 巻 3 号 138～188 頁にある。ETIAS 規則(EU) 2018/1240 の参考訳は、法と情報雑誌 4 巻 3 号 42～137 頁にある。参考訳入国／出国システム(EES)規則(EU) 2017/2226 の参考訳は、法と情報雑誌 3 巻 3 号 201～300 頁にある。規則(EU) 2018/1860 の参考訳は、法と情報雑誌 4 巻 4 号 69～88 頁にある。規則(EU) 2018/1861 の参考訳は、法と情報雑誌 4 巻 4 号 89～146 頁にある。

理事会決定 2008/615/JHA の参考訳は、法と情報雑誌 2 巻 2 号 155～181 頁にある。理事会決定 2008/616/JHA の参考訳は、法と情報雑誌 2 巻 9 号 116～200 頁にある。理事会枠組み決定 2002/584/JHA の参考訳は、法と情報雑誌 4 巻 5 号 185～206 頁にある。

規則(EU) 2018/1725 の参考訳は、法と情報雑誌 4 巻 1 号 1～81 頁にある。規則(EU) 2016/679（一般データ保護規則）の参考訳・再訂版は、法と情報雑誌 3 巻 5 号 1～114 頁にある。指令(EU) 2016/680 の参考訳は、法と情報雑誌 2 巻 1 号 141～169 頁にある。規則(EC) No 45/2001 の参考訳・改訂版は、法と情報雑誌 2 巻 5 号 111～146 頁にある。PNR 指令(EU) 2016/681 の参考訳は、法と情報雑誌 2 巻 3 号 119～155 頁にある。API 指令 2004/82/EC の参考訳は、法と情報雑誌 2 巻 5 号 60～70 頁にある。税関のための情報技術の利用に関する 2009 年 11 月 30 日の決定 2009/917/JHA の参考訳は、法と情報雑誌 2 巻 2 号 1～30 頁にある。委員会決定(EU) 2019/236 の参考訳は、法と情報雑誌 4 巻 3 号 189～197 頁にある。個人データの自動的な処理と関連する個人の保護に関する条約（ETS No.108）の参考訳は、法と情報雑誌 1 巻 4 号 1～20 頁にある。警察分野における個人データの利用に関する勧告 No. R (87) 15 の参考訳は、法と情報雑誌 1 巻 6 号 140～149 頁にある。

この参考訳を作成するに際しては、上記各参考訳の冒頭部分に掲記した参考文献を参考にした。

＊＊＊

刑事における警察協力及び法務上の協力の分野における シェンゲン情報システム（SIS）の構築、運営及び利用に関する、 理事会決定 2007/533/JHA を改正及び廃止し、 欧州議会及び理事会の規則(EC) No 1986/2006、委員会決定 2010/261/EU を廃止する 欧州議会及び理事会の 2018 年 11 月 28 日の規則(EU) 2018/1862

欧州議会及び欧州連合の理事会は、
欧州連合の機能に関する条約、並びに、とりわけ、その第 82 条第 2 副項(d)、第 85 条 1 項、第 87 条第 2 項(a)及び第 88 条第 2 項(a)に鑑み、
欧州委員会からの提案に鑑み、
立法案を国内議会に送付した後、
通常の立法手続に従って審議し[1]、
以下のとおりであるので、この規則を採択する。

(1) シェンゲン情報システム（SIS）は、欧州連合の枠組みの中に統合されたものとしてのシェンゲン協定の条項の適用のための基本的なツールを構成する。SIS は、職務権限を有する国内機関、とりわけ、国境警備、税関当局、移民当局、並びに、犯罪行為の防止、検知、捜査もしくは訴追または刑罰の執行について職責を負う機関の間における業務遂行上の協力を支援することにより、欧州連合の自由、安全及び法務の領域内における高いレベルの安全を維持することに貢献する重要な代償手段の 1 つである。

(2) SIS は、それらの国の共通国境の段階的廃止に関するベネルクス経済連合諸国、ドイツ連邦共和国及びフランス共和国の政府間の 1985 年 6 月 14 日のシェンゲン協定を実装する 1990 年 6 月 19 日の条約（シェンゲン協定実装条約）[2]の第 IV 款の条項により、最初に設置された。第 2 世代の SIS（SIS II）の開発は、理事会規則(EC) No 2424/2001[3]及び理事会決定 2001/886/JHA[4]により、欧州委員会に委任された。その後、SIS II は、欧州議会及び理事会の規則(EC) No 1987/2006[5]及び理事会決定 2007/533/JHA[6]によって構築された。SIS II は、シェンゲン協定実装条約により創設された SIS に置き換わった。

(3) SIS II が運用開始となった 3 年後、欧州委員会は、規則(EC) No 1987/2006 及び決定 2007/533/JHA に従い、システムの評価を実施した。2016 年 12 月 21 日、欧州委員会は、欧州議会及び理事会に対し、スタッフ作業文書を添えて、規則(EC) No 1987/2006 の第 24 条第 5 項、第 43 条第 3

[1] 欧州議会の 2018 年 10 月 24 日付け意見書（官報未登載）及び理事会の 2018 年 11 月 19 日付け決定。
[2] OJ L 239, 22.9.2000, p.19.
[3] 第 2 世代シェンゲン情報システム（SIS II）の開発に関する 2001 年 12 月 6 日の理事会規則(EC) No 2424/2001（OJ L 328, 13.12.2001, p.4）
[4] 第 2 世代シェンゲン情報システム（SIS II）の開発に関する 2001 年 12 月 6 日の理事会決定 2001/886/JHA（OJ L 328, 13.12.2001, p.1）
[5] 第 2 世代シェンゲン情報システム（SIS II）の構築、運営及び利用に関する欧州議会及び理事会の 2006 年 12 月 20 日の規則(EC) No 1987/2006（OJ L 381, 28.12.2006, p.4）
[6] 第 2 世代シェンゲン情報システム（SIS II）の構築、運営及び利用に関する欧州議会及び理事会の 2007 年 6 月 12 日の理事会決定 2007/533/JHA（OJ L 205, 7.8.2007, p.63）

項及び第 50 条第 5 項並びに決定 2007/533/JHA の第 59 条第 3 項及び第 66 条第 5 項に従い、第 2 世代シェンゲン情報システム（SIS II）の評価に関する報告書を提出した。これらの文書の中に示された勧告は、しかるべく、この規則に反映されなければならない。

(4) この規則は、欧州連合の機能に関する条約（TFEU）の第 3 部第 V 款第 4 章及び第 5 章の適用範囲内にある事項に関し、SIS の法的根拠を構成する。欧州議会及び理事会の規則(EU) 2018/1861[1]は、TFEU の第 3 部第 V 款第 2 章の適用範囲内にある事項に関し、SIS の法的根拠を構成する。

(5) SIS の法的根拠が別の法律文書によって構成されているということは、SIS が、そのような情報システムとして運営されるべき単一の情報システムを構成するという基本原則に対して影響を与えない。そのことは、補足情報の交換を確保するための SIRENE 事務局と呼ばれる単一の国内事務局のネットワークを含める。それゆえ、それらの法律文書の一定の条項は、同一のものでなければならない。

(6) SIS の目的、その技術アーキテクチャの一定の構成要素、及び、その資金調達を定め、そのエンドツーエンドの運営及び利用に関する規定を定め、そして、職責を定める必要がある。システムの中に入れられるデータの類型、そのデータが入れられ、処理される目的、そして、それらのデータを入れる基準も定められる必要がある。警報の削除、データへのアクセスの承認を受ける機関、生体データの利用を規律すること、並びに、データ保護及びデータ処理の規定を別に定めることも必要である。

(7) SIS の中にある警報は、ある者を識別するため、及び、実施される行動のために必要となる情報のみを含める。それゆえ、構成国は、それが必要なときは、警報と関連する補足情報を交換しなければならない。

(8) SIS は、1 つの中央システム（中央 SIS）及び複数の国内システムを含む。国内システムは、複数の構成国によって共有され得る SIS データベースの完全な複製物または部分的な複製物を含め得るものである。SIS が、保安及び実効的な国境管理を確保するための欧州内の最も重要な情報交換の道具であることを考慮すると、中央レベル及び国内レベルの業務遂行において、途切れることのない運営を確保する必要性がある。SIS の可用性は、中央レベル及び構成国レベルにおいて詳密な監視に服するものとしなければならず、また、エンドユーザのいかなる可用性喪失のインシデントも登録され、かつ、国内レベル及び欧州連合レベルにおいて、利害関係者に対して報告されなければならない。各構成国は、その構成国の国内システムのためのバックアップを設けなければならない。構成国は、多重化され、かつ、物理的及び地理的に区分された接続点をもつことにより、中央 SIS との間の途切れることのない接続性も確保しなければならない。中央 SIS 及び通信インフラは、1 日 24 時間、週 7 日間の SIS の稼働が確保されるような態様により運営されなければならない。それゆえ、欧州議会及び理事会の規則(EU) 2018/1726[2]によって設置された自由、安全及び法務の領域における大規模 IT システムの業務運営管理のための欧州連合局

[1] 国境検問の分野におけるシェンゲン情報システム（SIS）の構築、運営及び利用に関する、並びに、シェンゲン協定実装条約を改正し、及び、規則(EC) No 1987/2006 を廃止する欧州議会及び理事会の 2018 年 11 月 28 日の規則(EU) 2018/1861（この官報の 14 頁参照）

[2] 自由、安全及び法務の領域における大規模 IT システムの業務運営管理のための欧州連合局（eu-LISA）に関する、並びに、規則(EC) No 1987/2006 及び理事会決定 2007/533/JHA を改正し、規則(EU) No 1077/2011 を廃止する欧州議会及び理事会の 2018 年 11 月 14 日の規則(EU) 2018/1726（OJ L 295, 21.11.2018, p.99）

（「eu-LISA」）は、独立の影響評価及び費用対効果分析に従い、SIS の途切れることのない可用性を強化するための技術ソリューションを実装しなければならない。

(9) 警報によって求められる行動に関する補足情報の交換のための詳細な規則を定めるマニュアル（「SIRENE マニュアル」）を維持管理する必要性がある。SIRENE 事務局は、迅速かつ効率的な態様によるそのような情報の交換を確保しなければならない。

(10) 警報の中で指示された執るべき行動に関する情報を含め、補足情報の効率的な交換を確保するため、利用可能な資源及び利用者の訓練並びに他の SIRENE 事務局から受けた照会のための応答時間に関する要件を定めることにより、SIRENE 事務局の稼働を強化することが適切である。

(11) 構成国は、その構成国の SIRENE 事務局の職員が、その職務を遂行するために必要となる言語能力並びに関連する法律及び手続規則の知識をもつことを確保しなければならない。

(12) SIS の稼働から全面的に利益を享受できるようにするため、構成国は、エンドユーザ及び SIRENE 事務局の職員が、データセキュリティ、データ保護及びデータの品質に関するものを含め、定期的に訓練を受けることを確保しなければならない。SIRENE 事務局は、訓練計画の策定に関与しなければならない。可能な範囲内で、SIRENE 事務局は、少なくとも年 1 回、他の SIRENE 事務局との間の職員の交替も定めなければならない。構成国は、職員の交替によって技能及び経験が喪失することを避けるための適切な措置を講ずることが推奨される。

(13) SIS の中心的なコンポーネントの業務運営管理は、eu-LISA によって実施される。eu-LISA が、中央 SIS 及び通信インフラの業務運営管理の全ての側面を包摂する必要な資金及び人的資源を投ずることを可能とするため、この規則は、とりわけ、補足情報の交換の技術的側面に関し、その職務を詳細に定めなければならない。

(14) SIS の中に入れられるデータの正確性についての構成国の職責を妨げることなく、また、品質の調整者としての SIRENE 事務局の役割を妨げることなく、eu-LISA は、中央データ品質監視ツールを導入することにより、データの品質を強化することについて職責を負わなければならず、かつ、欧州委員会及び構成国に対し、定期的に、報告書を提出しなければならない。欧州委員会は、欧州議会及び理事会に対し、対処されたデータ品質上の問題に関し、報告しなければならない。SIS 内のデータの品質を更に向上させるため、eu-LISA は、国内訓練組織に対し、並びに、可能な範囲内において、SIRENE 事務局及びエンドユーザに対し、SIS の利用に関する訓練も提供しなければならない。

(15) SIS の利用をより良く監視できるようにするため、及び、犯罪行為に関する傾向を分析するため、eu-LISA は、データの完全性を損なうことなく、構成国、欧州議会、理事会、欧州委員会、Europol、Eurojust 及び欧州国境沿岸警備局に対して統計を報告するための最新の能力を開発できるものとすべきである。それゆえ、中央リポジトリが設置される。そのリポジトリの中に保持される統計またはそのリポジトリから得られる統計は、いかなる個人データも含めてはならない。構成国は、この規則に基づき、監督機関と欧州データ保護監督官との間の協力の枠組みの中におけるアクセスの権利、不正確なデータの訂正の権利及び違法に記録保存されたデータの削除の権利の行使に関する統計を送付する。

(16) エンドユーザが、警報に基づいて即座に決定の通知を受けることを可能とするため、新たなデータ類型が SIS の中に導入されなければならない。それゆえ、識別を容易にし、かつ、複数の識別名を検知するため、そのような情報を利用可能なときは、警報は、関係する個人の身分証明文書の参照またはその文書の番号、及び、可能なときはカラーで、その文書の複製物を含めなけれ

ばならない。

(17) 職務権限を有する機関は、それが厳格に必要な場合、刺青、傷跡または瘢痕のような、個人の変更されない、特定の、客観的で物理的な特徴と関連する個別の情報を SIS の中に入れることができるものとすべきである。

(18) 誤った該当ありのリスク及び無用な業務遂行活動をミニマム化するため、警報を作成する際、それが利用可能なときは、全ての関連データ、とりわけ、関係する個人の名が挿入されなければならない。

(19) その検索が適法であるか否かを確認するため、データ処理の適法性を監視するため、国内システムの適正な稼働を自己監視し、確保するため、並びに、データの完全性及び安全性のための履歴（ログ）の保存を除き、SIS は、検索を実施するために使用されるいかなるデータも記録保存してはならない。

(20) SIS は、関係する個人の信頼できる識別を補助するため、生体データの処理を許容しなければならない。SIS の中への写真、顔画像または指紋検査データの入力、及び、そのようなデータの利用は、求められる目的のために必要なところに限定されなければならず、欧州連合法によって承認されなければならず、児童の最善の利益を含め、基本的な権利を尊重しなければならず、かつ、この規則に定めるデータ保護に関する関連条項を含め、データ保護に関する欧州連合法に従うものでなければならない。同様の観点から、誤認から生ずる不都合を避けるため、SIS は、適切な安全性確保措置に服し、個々のデータ類型について、特に掌紋について、関係する個人の同意を獲得することに服し、そして、その個人データが適法に処理され得る目的という厳格な制限に服し、その識別子が濫用された個人に関するデータの処理も許容されなければならない。

(21) 欧州議会及び理事会の指令(EU) 2016/680[1]の第 4 条、並びに、欧州議会及び理事会の規則(EU) 2016/679[2]の第 5 条に定める基本原則に従い、エンドユーザが、毎回、国内警察データベースまたは移民データベース内の検索を実施する権利をもち、それと並行して、彼らが SIS も検索できるようにするため、構成国は、必要な技術上の手配を行わなければならない。その技術的な手配は、SIS が、域内国境のない領域における重要な代償手段として機能し、かつ、犯罪の国境を越える局面及び犯罪者のモビリティにより良く対応することを確保するものでなければならない。

(22) この規則は、識別の目的及び確認の目的のための指紋検査データ、写真及び顔画像の利用のための条件を定めなければならない。顔画像及び写真は、識別の目的のために、通常の国境入国地点の過程の中に限り、最初に使用されるものとしなければならない。そのような利用は、欧州委員会によるその技術の可用性、信頼性及び成熟性を確認する報告に服さなければならない。

(23) SIS 内に自動化された指紋識別サービスを導入することは、理事会決定 2008/615/JHA[3]及び理事会決定 2008/616/JHA[4]に定める指定された国内 DNA データベースシステム及び自動化された

---

[1] 犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行の目的のための職務権限を有する機関による個人データの処理と関連する自然人の保護、並びに、そのデータの支障のない移動に関する、並びに、理事会枠組み決定 2008/977/JHA を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の指令(EU) 2016/680（OJ L 119, 4.5.2016, p.89）

[2] 個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）（OJ L 119, 4.5.2016, p.1）

[3] とりわけテロリズム及び国境を越える犯罪との闘いにおける国境を越える協力の拡大に関する 2008 年 6 月 23 日の理事会決定 2008/615/JHA（OJ L 210, 6.8.2008, p.1）

[4] とりわけテロリズム及び国境を越える犯罪との闘いにおける国境を越える協力の拡大に関する理事会決定 2008/615/JHA の実装に関する 2008 年 6 月 23 日の理事会決定 2008/616/JHA（OJ L 210, 6.8.2008, p.12）

指紋識別システムへの国境を越えるオンラインの相互アクセスに関する既存のプリュムの仕組みを補完する。SIS の指紋検査データ検索は、加害者の能動的な検索を許容する。それゆえ、SIS は、その指紋検査データの持ち主が、重大犯罪またはテロリズム行為の非常に高度な蓋然性のある者として特定され得ることを条件として、未認知加害者の指紋データを SIS の中にアップロードすることを可能としなければならない。侵害行為のために使用された武器またはその他の対象物上で指紋検査データが発見された場合が特にそのような場合である。その指紋検査データが犯罪現場に存在しているということだけでは、その指紋が加害者の指紋検査データであるとの高度の蓋然性を示すものと判断してはなたない。関連する別の国内データベース、欧州連合のデータベースまたは国際的なデータベースからのデータを基礎として容疑者の同一性が確認され得ないということが、そのような警報の作成のためのもう 1 つの前提条件とされなければならない。指紋検査データの検索が合致の可能性を導くことを条件として、構成国は、容疑者が SIS 中に記録保存された指紋の保有者であるか否かを確認するため、専門家の関与により、更に検査を実施しなければならない。その手続は、国内法に従う。そのような識別は、捜査に大きく貢献し得るものであり、逮捕のための全ての条件に適合している限り、逮捕を導き得るものである。

(24) その指紋検査データが重大犯罪またはテロリスト犯罪の加害者に属するという高度の蓋然性が確認され得るときは、そのような検索が関連する国内指紋データベースの中で同時に実施されることを条件として、犯罪現場において発見された指紋または掌紋の完全なセットまたは部分的なセットのある SIS 中に記録保存された指紋検査データの検索が許容されなければならない。潜在指紋検査データを含め、生体データの記録保存に適用される品質基準を確認することに特別の注意が払われなければならない。

(25) 他の手段によっては個人の同一性を確認できない場合、識別を試みるために、指紋検査データが使用されなければならない。指紋検査データを使用することによる個人の識別は、全ての事件において許容されなければならない。

(26) 明確に定義された指紋検査データが利用できない場合において、警報の中に DNA プロファイルを付加できるものとすべきである。DNA プロファイルは、承認を受けた利用者のみがアクセス可能なものとしなければならない。DNA プロファイルは、直接の親、子、兄弟姉妹の DNA プロファイルの使用を許容することによる場合を含め、保護を要する失踪者及び特に失踪児童の識別を容易にするものでなければならない。DNA データは、失踪者の識別のために必要なミニマムの情報のみを含めるものとしなければならない。

(27) DNA プロファイルは、この規則に定める目的のために識別が必要かつ比例的な場合に限り、SIS から検索されるものとしなければならない。DNA プロファイルは、それが SIS の中に入れられた目的以外の目的のために検索または処理してはならない。この規則に定めるデータ保護の規定及びデータの安全性の規定が適用されなければならない。それが必要なときは、誤合致、ハッキング及び第三者による無権限の共有のリスクを避けるため、DNA プロファイルを利用する場合における追加的な安全性確保措置が設けられなければならない。

(28) SIS は、身柄引渡の目的のための逮捕のために手配された者及び引渡の目的のための逮捕のために手配された者に関する警報を含めるものとしなければならない。警報に加え、身柄引渡手続及び引渡手続のために必要な SIRENE 事務局を介する補足情報の交換を定めることが適切である。とりわけ、理事会枠組み決定 2002/584/JHA[1]の第 8 条に示すデータが SIS の中で処理され

[1] 欧州逮捕令状及び構成国間における身柄引渡手続に関する 2002 年 6 月 13 日の理事会枠組み決定 2002/584/JHA（OJ L 190, 18.7.2002, p.1）

なければならない。業務遂行上の理由により、欧州逮捕令状の対象者である者が集中的かつ能動的に検索され、かつ、個々具体的な検索業務に関与しないエンドユーザが結果の成功を危険に晒し得る場合、発行構成国は、法務当局の承認の下において、逮捕のための既存の警報を一時的に利用禁止とすることが適切である。そのような警報の一時的な使用禁止は、原則として、48 時間を超えてはならない。

(29) 欧州逮捕令状に基づく身柄引渡しの目的のため、及び、引渡しの目的のために入れられた追加データの翻訳文を SIS に付加できるものとすべきである。

(30) SIS は、彼らの保護を確保するため、または、公共の安全もしくは公共の秩序に対する脅威を防止するため、失踪者に関する警報または旅行が阻止される必要性のある脆弱な者に関する警報を含めなければならない。児童の場合、それらの警報及びそれに対応する手続は、欧州連合基本権憲章の第 24 条及び 1989 年 11 月 20 日の児童の権利に関する国際連合条約の第 3 条に従い、児童の最善の利益を与えなければならない。法務当局を含め、職務権限を有する機関による警報に従った行動及び決定は、児童保護機関と協力して行われなければならない。失踪児童に関する国内ホットラインは、該当するときは、通知を受けるものとしなければならない。

(31) 保護の下に置かれる必要のある失踪者に関する警報は、職務権限を有する機関からの要請に応じて入れられなければならない。構成国の収容施設から失踪した全ての児童は、SIS 中の失踪者に関する警報の対象者とされなければならない。

(32) 親による児童の連れ去りのリスクに直面している児童に関する警報は、国内法に基づき親権に関する事項の管轄権をもつ法務当局を含め、職務権限を有する機関の要請に応じて、SIS の中に入れられなければならない。親による児童の連れ去りのリスクに直面している児童に関する警報は、そのリスクが具体的なものであり、かつ、明白であり、かつ、限定された状況におけるものである場合に限り、SIS の中に入れられるものとしなければならない。それゆえ、厳格かつ適切な基準が定められる必要性がある。ある児童がある構成国から直ちにかつ違法に連れ去られる可能性があるという具体的かつ明白なリスクが存在するか否かを検討する際、職務権限を有する機関は、その児童の心身の状態及びその児童が曝されている環境を考慮に入れなければならない。

(33) この規則は、旅行が阻止される必要性のある一定の類型の脆弱な者に関する新たな類型の警報を定めなければならない。その年齢のゆえに、無能力である者、または、その家族環境が保護を要求している者は、脆弱であると判断されなければならない。

(34) ある構成国の領土からの連れ去される、または、退去させられる具体的かつ明白なリスクが存在する場合、彼ら自身の保護のために旅行が阻止される必要性のある児童に関する警報が SIS の中に入れられなければならない。その旅行が、人身取引の被害者となるリスク、強制婚姻もしくは女性器切除またはそれ以外の性暴力の被害者となるリスク、テロリスト犯罪の被害者または加担者となるリスク、武装グループへ徴兵または加入させられるリスク、または、兵站の活動に加担させられるリスクに彼らを直面させる場合、そのような警報が入れられる。

(35) その旅行が、人身取引または性暴力の被害者となるリスクに彼らを直面させる場合、彼ら自身の保護のために旅行が阻止される必要性のある脆弱性のある成人に関する警報が入れられなければならない。

(36) 厳格かつ適正な安全性確保措置を保障するため、旅行が阻止される必要性のある脆弱性のある児童またはそれ以外の脆弱性のある者に関する警報は、国内法の下においてそれが要求される場合、法務当局の決定または法務当局から承認を受けた職務権限を有する機関による決定の後、

SIS の中に入れられるものとしなければならない。

(37) 執られるべき新たな行動は、発行構成国が詳細情報を入手するために、ある者を停止させ、質問することができることの導入でなければならない。この行動は、明確な徴証を基礎として、ある者が、枠組み決定 2002/584/JHA の第 2 条第 1 項及び第 2 項に示すいずれかの侵害行為の実行を意図している容疑または実行している容疑がある場合、枠組み決定 2002/584/JHA の第 2 条第 1 項及び第 2 項に示すいずれかの侵害行為により有罪判決を受けた者に対し、拘禁刑または拘禁命令を執行するために更に情報が必要な場合、または、彼もしくは彼女がそれらの侵害行為のいずれかを実行すると信ずる理由が存在する場合において、適用されなければならない。また、この執られるべき行動は、既存の法律上の共助の仕組みを妨げてはならない。それは、更なる行動に関して決定するための十分な情報を供給しなければならない。この新たな行動は、その者の捜索にも彼または彼女の逮捕にも及ぶものとしてはならない。欧州議会及び理事会の指令 2013/48/EU[1]に従って弁護士へのアクセスをもつ容疑者及び被訴追者の権利を含め、欧州連合法及び国内法に基づく容疑者及び被訴追者の手続上の権利は、維持されなければならない。

(38) 刑事手続における差押えまたは証拠としての使用のための対象物に関する警報の場合、関係する対象物は、対象物が差し押さえられる場合の条件、とりわけ、その対象物がその対象物の権利の保有者のある場合の条件、及び、どの条件に従うかを定める国内法に従って差し押さえられなければならない。

(39) SIS は、ユニークな識別番号によって識別及び検索され得る情報技術の項目のような、価値の高い新たな類型の対象を含めなければならない。

(40) 刑事手続における差押えまたは証拠としての使用のための文書に関して SIS の中に入れられる警報に関し、「偽造」との用語は、偽造文書及び模造文書の両者を含むものとして解釈されなければならない。

(41) 警報に基づいて執られるべき行動がその構成国の領土上においては行われないという効果のために、構成国が、フラグをたてて、警報に指示を付加できるものとすべきである。身柄引渡しの目的のための逮捕のために警報が入れられる場合、この規則のいかなる条項も、枠組み決定 2002/584/JHA に含まれている条項の適用から免脱するため、または、その適用を阻止するために解釈してはならない。欧州逮捕令状の不執行のために警報にフラグを付加する決定は、同枠組み決定に含まれている拒否の根拠のみを基礎とするものでなければならない。

(42) フラグが付加され、かつ、身柄引渡しのための逮捕が手配された者の所在が認知された場合、その者の所在は、常に、発付法務当局に対して通知されなければならず、その法務当局は、枠組み決定 2002/584/JHA の条項により職務権限を有する法務当局に対して欧州逮捕令状を送付することを決定できる。

(43) SIS 中の警報と警報との間のリンクを構成国が設けることができるものとすべきである。複数の警報間のリンクの設置は、執られるべき行動、警報の見直し期間、または、警報へのアクセスの権利に対し、いかなる影響も与えてはならない。

(44) 警報は、それらの警報が入れられた個別の目的を満たすために要する期間内だけ、SIS の中に保存されるものとしなければならない。異なる類型の警報の評価期間は、それらの目的に照らし、

[1] 刑事手続及び欧州逮捕令状手続における弁護士へのアクセスの権利に関する、並びに、自由の剥奪について第三者に通知させる権利、及び、自由の剥奪の間に第三者及び領事機関と連絡をとる権利に関する欧州議会及び理事会の 2013 年 10 月 22 日の指令 2013/48/EU（OJ L 294, 6.11.2013, p.1）

適切なものでなければならない。個人に関する警報とリンクされている対象物に関する警報は、その者の警報が保存される期間内に限り、保存されるものとしなければならない。個人に関する警報を保持する決定は、包括的な個別評価を基礎としなければならない。構成国は、所定の見直し期間内に、個人に関する警報及び対象物に関する警報を見直さなければならず、かつ、保持期間が延長された警報の数に関する統計を保存しなければならない。

(45) SIS の中に警報を入れること、及び、SIS の中にある警報の期限を延長することは、具体的な案件が、SIS の中に警報を入れる根拠を満たすために十分な適切性、関連性及び重要性のあるものであるか否かの検討を含む比例性の要件に服するものとしなければならない。テロリスト行為が関係する場合、SIS 内の警報の根拠として十分な適切性、関連性及び重要性があると判断されるべきである。公共の安全または国家安全保障上の理由に関し、構成国は、それが公的調査または法律上の調査、捜査または手続の妨げとなり得るおそれがある場合、例外として、SIS の中に警報を入れることを控えることが認められるものとしなければならない。

(46) 警報の削除に関する規定を設ける必要性がある。警報は、それが入れられた目的を達成するために要する期間に限り、保存されるものとしなければならない。警報がその目的を満たした時点の決定における構成国の実務の格差を考慮し、警報が削除されなければならない場合を決定するために、個々の類型の警報毎に詳細な基準を定めることが適切である。

(47) SIS のデータの完全性は、最も重要なものである。それゆえ、データのエンドツーエンドの安全性を確保するため、中央レベル及び国内レベルにおいて、SIS のデータを処理するための適切な安全性確保措置が定められなければならない。データ処理に関与する機関は、この規則のセキュリティの要件によって拘束され、統一的なインシデント通報手続に服するものとしなければならない。それらの機関の職員は、適切に訓練を受け、かつ、それに関する違反行為及び制裁について説明を受けるものとしなければならない。

(48) SIS の中で処理されるデータ及びこの規則によって交換される関連補足情報は、第三国または国際機関に対して移転され、または、利用できるようにされてはならない。

(49) 差押えのために、構成国内において、関係するどの運送手段が捜索を受けているかをそれらの機関が確認できるようにするため、自動車、船舶及び航空機の登録について職責を負う機関に対し、SIS へのアクセスを与えることが適切である。差押えのために、構成国内において、関係するどの武器が捜索を受けているか、または、登録を求めている者に関する警報が存在するか否かをそれらの機関が確認できるようにするため、武器の登録について職責を負う機関に対し、SIS へのアクセスを与えることが適切である。

(50) SIS への直接のアクセスは、職務権限を有する政府機関に対してのみ与えられるものとしなければならない。このアクセスの対象は、それぞれの運送手段と関係する警報、並びに、その運送手段の登録文書もしくは登録番号、または、武器及びその登録を求めている者に限定されなければならない。SIS 内の全ての該当ありは、そのような機関から警察当局に対して報告されなければならず、その警察当局は、SIS 内の特別の警報に沿って更に行動を執らなければならず、かつ、発行構成国に対し、SIRENE 事務局を介して、その該当ありを通知しなければならない。

(51) この規則に定めるより細目的な規定を妨げることなく、指令(EU) 2016/680 によって採択された国内法、規則及び行政規則は、テロリスト行為またはそれ以外の重大犯罪行為の防止、検知、捜査または訴追の目的のため、または、刑罰の執行の目的のために職務権限を有する国内機関によって、収集及び送信を含め、この規則に基づいて実施される個人データの処理に適用されなけ

ればならない。テロリスト行為またはそれ以外の重大犯罪行為の防止、捜査、検知または捜査、または、刑罰の執行について職責を負う職務権限を有する国内機関による SIS の中に入れられたデータへのアクセス及びそのようなデータを検索する権利は、この指令の全ての関連条項、並びに、国内法へ国内法化されたものとしての指令(EU) 2016/680 の関連条項、とりわけ、指令(EU) 2016/680 に示す監督機関による監視に服さなければならない。

(52) 個人データの処理に関してこの規則に定めるより細目的な規定を妨げることなく、テロリスト行為またはそれ以外の重大犯罪行為の防止、検知、捜査または訴追の目的のために職務権限を有する国内機関によってそのような処理が実施される場合を除き、規則(EU) 2016/679 は、この規則に基づく構成国による個人データの処理に適用されなければならない。

(53) 欧州議会及び理事会の規則(EU) 2018/1725[1]は、この規則に基づくそれらの機関の職責を実施する際、欧州連合の機関及び組織による個人データの処理に適用されなければならない。

(54) 欧州議会及び理事会の規則(EU) 2016/794[2]は、この規則に基づく Europol による個人データの処理に適用されなければならない。

(55) Eurojust の国内構成員及びその補佐官によって SIS の中で実施された検索により、構成国によって入れられた警報の存在が明らかにされた場合、Eurojust は、要求された行動を執ることができない。それゆえ、Eurojust は、関係する構成国に対し、その案件をその構成国がフォローアップできるようにするため、通知する。

(56) SIS を利用する場合、職務権限を有する機関は、そのデータが処理される者の尊厳と完全性が尊重されることを確保しなければならない。この規則の目的のための個人データの処理は、性、人種的または民族的な出自、信教及び信条、障害、年齢または性的指向のような理由に基づくそれらの者に対する差別を生じさせてはならない。

(57) 機密性が関係する範囲内において、理事会規則(EEC, Euratom, ECSC) No 259/68[3]に定める欧州連合の官吏の職員規則及び欧州連合のその他の公務員の雇用条件（「職員規則」）は、SIS との関係において雇用され、業務に従事する官吏またはそれ以外の公務員に適用されなければならない。

(58) 構成国及び eu-LISA の両者は、セキュリティ上の義務の実装を容易にするためのセキュリティ計画を維持管理しなければならず、かつ、セキュリティ上の問題に対して共通の観点から対処するため、相互に協力しなければならない。

(59) 規則(EU) 2016/679 及び指令(EU) 2016/680 に示す独立の国内監督機関（「監督機関」）は、補足情報の交換を含め、この規則に基づく構成国による個人データの処理の適法性を監視しなければならない。監督機関は、その職務を遂行するための十分な資源を与えられなければならない。SIS の中に記録保存された彼らの個人データへのアクセス、その訂正及び削除のためのデータ主体の権利、国内裁判所における事後的な救済、並びに、判決の相互承認が定められなければ

---

[1] 欧州連合の機関、組織、事務局及び部局による個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725（OJ L 295, 21.11.2018, p.39）

[2] 欧州連合法執行協力局（Europol）の設置に関する、並びに、理事会決定 2009/371/JHA、理事会決定 2009/934/JHA、理事会決定 2009/935/JHA、理事会決定 2009/936/JHA 及び理事会決定 2009/968/JHA を廃止する欧州議会及び理事会の 2016 年 5 月 11 日の規則(EU) 2016/794（OJ L 135, 24.5.2016, p. 53）

[3] OJ L 56, 4.3.1968, p.1

ならない。構成国からの年次統計を要求することが適切である。

(60) 監督機関は、少なくとも 4 年に 1 回、国際的な監査基準に従い、その監督機関の構成国の国内システムにおけるデータ処理業務の監査が実施されることを確保しなければならない。その監査は、その監督機関によって実施されなければならず、または、その監督機関は、独立のデータ保護監査人に対して監査を直接に命じなければならない。独立の監査人は、関係する監督機関の監督及び職責の下にあるものとされなければならず、それゆえ、その監督機関は、監査人自身に対して指示を与え、かつ、監査のための明確に定義された目的、適用範囲及び手法、並びに、監査及びその最終結果と関係する指導及び監督を提供しなければならない。

(61) 欧州データ保護監督官は、この規則に基づく個人データの処理との関係において、欧州連合の機関及び組織の活動を監視しなければならない。欧州データ保護監督官及び監督機関は、SIS の監視において、相互に協力しなければならない。

(62) 欧州データ保護監督官は、生体データの専門知識をもつ者による補佐を含め、この規則に基づき欧州データ保護監督官に託された職務を満たすための十分な資源を与えられなければならない。

(63) 欧州議会及び理事会の規則(EU) 2016/794 は、Europol が、テロリズム及び重大犯罪との闘いにおいて職務権限を有する国内機関によって実施される活動及びそれらの機関の協力を支援し、強化すること、並びに、分析及び脅威評価を提供することを定めている。失踪者に関する警報への Europol のアクセスの権利を拡大することは、オンラインによる場合を含め、人身取引及び児童の性的虐待と関係する包括的な業務遂行上及び分析上の成果を国内法執行機関に対して提供するための Europol の能力を更に向上させるものでなければならない。このことは、潜在的な犠牲者を保護するため、及び、加害者の捜査のため、それらの犯罪行為のより良い防止に貢献するであろう。Europol の欧州サイバー犯罪センターもまた、旅行中の性犯罪者及びオンラインの児童の性的虐待の場合を含め、Europol が失踪者に関する警報へのアクセスをもつことからの利益を享受し得る。そのオンラインの場において、加害者は、しばしば、失踪者として登録されているかもしれない児童へのアクセスをもち、または、そのような児童へのアクセスを獲得可能であると主張している。

(64) （特に彼らの移動の監視が重要な場合において）とりわけ、外国人テロリスト戦闘員に関し、テロリズムに関する情報共有の間隙を埋めるため、構成国は、Europol との間におけるテロリズム関連活動に関する情報を共有することが推奨される。この情報共有は、関係する警報に関し、Europol との間の補足情報の交換を介して実施されなければならない。その目的のために、Europol は、通信インフラとの接続を設けなければならない。

(65) この規則及び規則(EU) 2016/794 に定めるデータ保護の基準が遵守されることを条件として、Europol が SIS を包括的に使用可能とするため、SIS のデータの処理及びダウンロードに関して Europol に適用される明確な規定を定める必要性がある。SIS の中において Europol によって実施された検索により、構成国によって入れられた警報の存在が明らかにされた場合、Europol は、求められた行動を執ることができない。それゆえ、Europol は、関係する構成国に対し、当該構成国がその案件をフォローアップできるようにするため、それぞれの SIRENE 事務局との間の補足情報の交換を介して、情報提供しなければならない。

(66) 欧州議会及び理事会の規則(EU) 2016/1624[1]は、同規則の目的のために、国境検問、国境監視及び帰国に関する業務遂行計画の中で定められる業務遂行上の目的を満たすためにその照会

[1] 欧州国境沿岸警備に関する、並びに、欧州議会及び理事会の規則(EU) 2016/399 を改正し、欧州議会及び理事会の規

が必要である場合、欧州国境沿岸警備局によって配置される同規則の第 2 条(8)に示すチームの構成員に対し、欧州連合のデータベースを照会することをホスト構成国が承認すべきことを定めている。欧州連合のそれ以外の部局、とりわけ、欧州庇護支援局及び Europol もまた、移民管理支援チームの一員として、それらの欧州連合の部局の職員ではない専門家を配置できる。同規則の第 2 条(8)及び(9)に示すチームを配置する目的は、要請元構成国に対し、特に、尋常ではない移民上の問題を直面している構成国に対し、技術上及び業務遂行上の強化を提供することである。同規則の第 2 条(8)及び(9)に示すチームに関し、それらのチームの職務を果たすため、それらのチームは、中央 SIS に接続されている欧州国境沿岸警備局の技術インタフェイスを介して、SIS へのアクセスを要求する。規則(EU) 2016/1624 の第 2 条(8)及び(9)に示すチームによって、または、職員のチームによって実施された SIS 内の検索により、ある構成国によって入れられた警報の存在が明らかにされた場合、そのチームの構成員またはその職員は、ホスト構成国からそのようにすることの承認を受けている場合を除き、求められた行動を執ることができない。それゆえ、ホスト構成国は、その案件をそのホスト構成国がフォローアップできるようにするため、情報提供を受けるものとしなければならない。そのホスト構成国は、発行構成国に対し、補足情報の交換を介して、その該当ありを通知しなければならない。

(67) その技術的であり、高度に詳細であり、かつ、頻繁に変化する性質に鑑み、SIS の一定の側面は、この規則によって独占的に包摂され得ない。それらの側面は、例えば、データの入力、データのアップデート、削除及び検索、データの品質に関する規則、並びに、生体データに関する規則、最長期間内で警報が無効となる日を定め、警報の互換性及び優先順序、複数の警報間のリンクに関する規則、補足情報の交換に関する規則を含む。それゆえ、欧州委員会に対し、それらの側面に関する実装権限が与えられなければならない。警報の検索に関する技術規則は、国内アプリケーションの円滑な運営を考慮に入れなければならない。

(68) この規則の実装に関する統一的な条件を確保するため、欧州委員会に対し、実装権限が与えられなければならない。それらの権限は、欧州議会及び理事会の規則(EU) No 182/2011[1]に従って行使されなければならない。この規則及び規則(EU) 2018/1861 に基づく実装行為の採択のための手続も同じでなければならない。

(69) 透明性を確保するため、この規則による SIS の運営開始の 2 年後、eu-LISA は、それらのセキュリティを含め、中央 SIS 及び通信インフラの技術的な稼働に関する報告書、並びに、補足情報の 2 国間交換及び多国間交換に関する報告書を作成する。全体評価書は、4 年毎に、欧州委員会によって発行されなければならない。

(70) SIS の円滑な稼働を確保するため、欧州委員会に対し、TFEU の第 290 条に従い、差押えの対象物に関する警報の下で捜索され、刑事手続において証拠として使用される対象物の新たな下位類型に関する行為を採択し、並びに、通常の国境入国地点の過程以外の、写真及び顔画像が個人の識別のために使用され得る状況の決定に関する行為を採択する権限が委任されなければならない。その準備作業の間、専門家レベルのものを含め、欧州委員会が適切に協議を実施すること、及び、より良い立法に関する 2016 年 4 月 13 日の機関間合意[2]に定める基本原則に従っ

則(EC) 863/2007、理事会規則(EC) No 2007/2004 及び理事会決定 2005/267/EC を廃止する欧州議会及び理事会の 2016 年 9 月 14 日の規則(EU) 2016/1624（OJ L 251, 16.9.2016, p. 1）

[1] 欧州委員会の実装権限の行使の構成国による監督のための仕組みに関する規則及び一般原則を定める欧州議会及び理事会の 2011 年 2 月 16 日の規則(EU) No 182/2011（OJ L 55, 28.2.2011, p.13）

[2] OJ L 123, 12.5.2016, p.1.

てそれらの協議が実施されることは、特に重要なことである。とりわけ、委任される行為の準備における平等な関与を確保するため、欧州議会及び理事会は、構成国の専門家と同時に、全ての文書を受け取り、かつ、欧州議会及び理事会の専門家は、自動的に、委任される行為の準備を取り扱う欧州委員会の専門家グループの会合へのアクセスをもつ。

(71) この規則の目的、すなわち、欧州連合の情報システムの構築及び規制並びに関連する補足情報の交換は、構成国によっては十分に達成され得ず、それらの性質のゆえに、欧州連合のレベルでより良く達成され得るものであるので、欧州連合は、欧州連合条約（TEU）の第 5 条に定める補完性の原則に従い、措置を採択できる。同条に定める比例性の原則に従い、この規則は、その目的を達成するために必要となるところを越えることがない。

(72) この規則は、基本的な権利を尊重し、欧州連合基本権憲章によって認められた基本原則を尊重する。とりわけ、この規則は、欧州連合の領域内に居住する全ての者の安全な環境、及び、人身取引の被害者となり得る児童に対する特別の保護を確保することを求めつつ、欧州連合基本権憲章の第 8 条による個人データの保護を全面的に尊重する。児童と関係する案件においては、児童の最善の利益が第一次的に考慮されなければならない。

(73) TEU 及び TFEU に附属するデンマークの地位に関する議定書第 22 号の第 1 条及び第 2 条に従い、デンマークは、この規則の採択に参加せず、この規則によって拘束されることがなく、または、この規則の適用に服さない。この規則がシェンゲン協定を基礎とすることに鑑み、デンマークは、同議定書の第 4 条に従い、この規則に関して理事会が決定した後の 6 か月の期間内に、その国内法の中にこの規則を実装するか否かを決定する。

(74) TEU 及び TFEU に附属し、欧州連合の枠組みの中に統合されたシェンゲン協定の議定書第 19 号の第 5 条第 1 項並びに理事会決定 2000/365/EC[1]の第 8 条第 2 項に従い、英国は、この規則に参加する。

(75) TEU 及び TFEU に附属する議定書第 19 号の第 5 条第 1 項並びに理事会決定 2002/192/EC[2]の第 6 条第 2 項に従い、アイルランドは、この規則に参加する。

(76) アイスランド及びノルウェーに関しては、この規則は、シェンゲン協定の実装、適用及び発展へのアイスランド共和国及びノルウェー王国の参加に関する欧州連合の理事会並びにアイスランド共和国及びノルウェー王国の間で締結された協定[3]の意味におけるシェンゲン協定の条項の発展を構成し、それは、理事会決定 1999/437/EC[4]の第 1 条の G に示す領域の範囲内にある。

(77) スイスに関しては、この規則は、シェンゲン協定の実装、適用及び発展へのスイス連邦の参加に関する欧州連合、欧州共同体及びスイス連邦の間で締結された協定[5]の意味におけるシェンゲン協定の条項の発展を構成し、それは、理事会決定 2008/146/EC[6]の第 3 条を重畳的に適用して読み替えられる決定 1999/437/EC の第 1 条の G に示す領域の範囲内にある。

---

[1] シェンゲン協定の幾つかの条項に参加するためのグレートブリテン及び北アイルランド連合王国の要請に関する 2000 年 5 月 29 日の理事会決定 2000/365/EC（OJ L 131, 1.6.2000, p.43）

[2] シェンゲン協定の幾つかの条項に参加するためのアイルランドの要請に関する 2002 年 2 月 28 日の理事会決定 2002/192/EC（OJ L 64, 7.3.2002, p.20）

[3] シェンゲン協定の実装、適用及び発展へのアイスランド及びノルウェーの参加に関して欧州連合並びにアイスランド共和国及びノルウェー王国の間で締結された協定の適用のための一定の覚書に関する 1999 年 5 月 17 日の理事会決定 1999/437/EC（OJ L 176, 10.7.1999, p.31）

[4] OJ L 176, 10.7.1999, p.36.

[5] OJ L 53, 27.2.2008, p.52.

[6] シェンゲン協定の実装、適用及び発展へのスイス連邦の参加に関する欧州連合、欧州共同体及びスイス連邦の間で締

(78) リヒテンシュタインに関しては、この規則は、シェンゲン協定の実装、適用及び発展へのスイス連邦の参加に関する欧州連合、欧州共同体及びスイス連邦の間で締結された協定へのリヒテンシュタイン公国の加入に関する欧州連合、欧州共同体、スイス連邦及びリヒテンシュタイン公国の間の議定書 [1]の意味におけるシェンゲン協定の条項の発展を構成し、それは、理事会決定 2011/350/EU[2]の第 3 条を重畳的に適用して読み替えられる決定 1999/437/EC の第 1 条の G に示す領域の範囲内にある。

(79) ブルガリア及びルーマニアに関しては、この規則は、2005 年加入法の第 4 条第 2 項に意味におけるシェンゲン協定またはそれと関連する他の法規範を基礎とする行為を構成し、かつ、理事会決定 2010/365/EU[3]及び理事会決定(EU) 2018/934[10] を重畳的に適用して読み替えられなければならない。

(80) クロアチアに関しては、この規則は、2011 年加入法の第 4 条第 2 項に意味におけるシェンゲン協定またはそれと関連する他の法規範を基礎とする行為を構成し、かつ、理事会決定(EU) 2017/733[4]を重畳的に適用して読み替えられなければならない。

(81) キプロスに関しては、この規則は、2003 年加入法の第 3 条第 2 項に意味におけるシェンゲン協定またはそれと関連する他の法規範を基礎とする行為を構成する。

(82) この規則は、アイルランドに対するシェンゲン協定の適用に関する関連法律文書に定める手続に従って決定される日に、アイルランドに適用されなければならない。

(83) この規則は、SIS の実効性を増加させ、データ保護を強化し、そして、アクセスの権利を拡大する SIS の一連の改善を導入するものである。他の要素は変化する揺れの大きさをもつ技術の変更を要求するものであるが、これらの改善の一定の要素は、複雑な技術開発を必要としない。可能な限り速やかにシステムの改善をエンドユーザが利用できるようになることを可能とするため、この規則は、複数の段階において、決定 2007/533/JHA の改正を導入する。システムの多数の改善がこの規則の発効後直ちに適用されなければならず、それ以外の改善は、この規則の発効後 1 年または 2 年で適用されなければならない。この規則は、その発効後、3 年以内に、全面的に適用されなければならない。その適用の遅延を避けるため、この規則の段階的な実装は、詳密に監視されなければならない。

(84) 欧州議会及び理事会の規則(EC) No 1986/2006[5]、決定 2007/533/JHA 及び委員会決定 2010/261/

結された協定の、欧州共同体の代理としての締結に関する 2008 年 1 月 28 日の理事会決定 2008/146/EC（OJ L 53, 27.2.2008, p.1）

[1] OJ L 160, 18.6.2011, p.21.

[2] 域内国境における検問の廃止及び人の移動に関し、シェンゲン協定の実装、適用及び発展へのスイス連邦の参加に関する欧州連合、欧州共同体及びスイス連邦の間で締結された協定へのリヒテンシュタイン公国の加入に関する欧州連合、欧州共同体、スイス連邦及びリヒテンシュタイン公国の間の議定書の、欧州連合の代理としての締結に関する 2011 年 3 月 7 日の理事会決定 2011/350/EU（OJ L 160, 18.6.2011, p.19）

[3] ブルガリア共和国及びルーマニアにおけるシェンゲン情報システムと関連するシェンゲン協定の条項の適用に関する 2010 年 6 月 29 日の理事会決定 2010/365/EU（OJ L 166, 1.7.2010, p.17）

[10] ブルガリア共和国及びルーマニアにおけるシェンゲン情報システムと関連するシェンゲン協定の条項を発効させることに関する 2018 年 6 月 25 日の理事会決定(EU) 2018/934（OJ L 165, 2.7.2018, p.37）

[4] クロアチア共和国におけるシェンゲン情報システムと関連するシェンゲン協定の条項の適用に関する 2017 年 4 月 25 日の理事会決定(EU) 2017/733（OJ L 108, 26.4.2017, p.31）

[5] 自動車登録証明書の発行について職責を負う構成国の機関によrふ第 2 世代シェンゲン情報システム（SIS II）へのアクセスに関する欧州議会及び理事会の 2006 年 12 月 20 日の規則(EC) No 1986/2006（OJ L 381, 28.12.2006, p.1）

EU[1]は、この規則の全面適用の日から発効するものとして、廃止されなければならない。

(85) 欧州データ保護監督官は、欧州議会及び理事会の規則(EC) No 45/2001[2]の第 28 条第 2 項によって協議を行い、2017 年 5 月 3 日に意見書を提出した。

[1] 中央 SIS II 及び通信インフラのためのセキュリティ計画に関する 2010 年 5 月 4 日の委員会決定 2010/261/EU（OJ L 112, 5.5.2010, p.31）

[2] 欧州共同体の機関及び組織による個人データの処理と関連する個人の保護並びにそのデータの支障のない移動に関する欧州議会及び理事会の規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1）

第 I 章 総則的な条項

第 1 条 SIS の一般的な目的

SIS の目的は、構成国の領土における公共の安全及び公共政策の維持並びに安全の防護を含め、欧州連合の自由、安全及び法務の領域内における高いレベルの安全を確保すること、そして、このシステムを介して送付される情報を使用し、それらの構成国の領土上における個人の移動と関連する TFEU の第 3 部第 V 款第 4 章及び第 5 章の条項の適用を確保することにある。

第 2 条 対象事項

1. この規則は、個人及び対象物に関する SIS 内の警報の入力及び処理に関する条件及び手続、並びに、刑事における警察協力及び法務上の協力の目的のための補足情報及び追加データの交換に関する条件及び手続を定める。
2. この規則は、SIS の技術アーキテクチャに関する条項、構成国の職責並びに自由、安全及び法務の領域における大規模 IT システムの業務運営管理のための欧州連合局（eu-LISA）の職責に関する条項、データ処理に関する条項、関係する個人の権利に関する条項及び法的責任に関する条項も定める。

第 3 条 定義

この規則の目的のために、以下の定義が適用される：

(1) 「警報」とは、職務権限を有する機関が、指定された行動を執るために個人または対象物を識別できるようにする SIS の中に入れられたデータのセットのことを意味し；
(2) 「補足情報」とは、SIS の中に記録保存される警報データの一部を構成する情報ではないが、以下のとおり、SIRENE 事務局を介して交換される情報を意味し：
  (a) 警報を入れる際、構成国が相互に協議または情報提供できるようにするため；
  (b) 該当ありの後に、適切な行動を執ることができるようにするため；
  (c) 要求される行動を執ることができない場合；
  (d) SIS データの品質を取り扱う場合；
  (e) 警報の互換性及び優先度を取り扱う場合；
  (f) アクセスの権利を取り扱う場合。
(3) 「追加データ」とは、SIS の中にその者に関するデータが入れられた者が SIS 内の検索の実施の結果として発見された場合において、職務権限を有する機関が直ちに利用できるように SIS 内に記録され、SIS 内の警報と関係付けられたデータのことを意味し；
(4) 「個人データ」とは、規則(EU) 2016/679 の第 1 条第 1 号に定義する個人データのことを意味し；
(5) 「個人データの処理」とは、自動化された手段によるか否かを問わず、収集、記録、履歴保存、編集、構成、記録保存、修正もしくは変更、検索、参照、使用、送信による開示、配布、または、それら以外に利用可能にすること、整列もしくは結合、制限、削除もしくは破壊のような、

個人データまたは個人データのセットに関して遂行される業務遂行または業務遂行のセットのことを意味し；

(6) 「合致」とは、以下の段階が生ずることを意味し：
  (a) エンドユーザによって SIS の中で検索が実施され；
  (b) その検索により、別の構成国によって SIS の中に警報が入れられたことが明らかにされ；かつ、
  (c) SIS の中にある警報と関係するデータが検索データと合致する。

(7) 「該当あり」とは、以下の基準を満たす合致のことを意味し；
  (a) その該当ありが、以下によって確認されたこと；
    (i) エンドユーザ；または、
    (ii) 関係する合致が生体データの照合を基礎とするものであった場合、国内手続に従い、職務権限を有する機関；
    かつ、
  (b) 更に別の行動が要求されること；

(8) 「フラグ」とは、国内レベルにおける警報の有効性の停止であって、逮捕のための警報、失踪者及び脆弱性のある者に関する警報、並びに、慎重な検問、質問による検問及び個別の検問に関する警報に付加され得るもののことを意味し；

(9) 「発行構成国」とは、SIS の中に警報を入れた構成国のことを意味し；

(10) 「執行構成国」とは、該当ありの後、要求された行動を執る構成国またはその行動を執った構成国のことを意味し；

(11) 「エンドユーザ」とは、CS-SIS、N.SIS またはそれらの技術複製物を直接に検索することの承認を受けた職務権限を有する機関の職員のことを意味し；

(12) 「生体データ」とは、自然人の身体的または生理的な特徴と関連する個別の技術的処理から生ずる個人データであって、当該自然人のユニークな識別を可能とし、または、それを確認するもの、すなわち、写真、顔画像、指紋検査データ及び DNA プロファイルのことを意味し；

(13) 「指紋検査データ」とは、それらに含まれるそれらのユニークな特徴及び参照点のゆえに、個人の同一性に関する正確かつ決定的な照合を可能とする指紋及び掌紋に関するデータのことを意味し；

(14) 「顔画像」とは、自動化された生体データの照合において使用されるために十分な画像解像度及び品質をもつ顔のデジタル画像のことを意味し；

(15) 「DNA プロファイル」とは、人間の DNA の分析されたサンプルの非コード領域の 1 組の識別特徴、すなわち、様々な DNA 配置（遺伝子座）における特別な分子構造を示す符号コードまたは番号コードのことを意味し；

(16) 「テロリスト行為」とは、欧州議会及び理事会の指令(EU) 2017/541[1]の第 3 条ないし第 14 条に示す国内法に基づく行為、または、同指令によって拘束されない構成国に関しては、それらの行為のいずれかと均等な行為のことを意味し；

[1] テロリズムとの闘いに関する、並びに、理事会枠組み決定 2002/475/JHA を置き換え、理事会決定 2005/671/JHA を改正する欧州議会及び理事会の 2013 年 8 月 12 日の指令(EU)2017/541（OJ L 88, 31.3.2017, p.6）

(17) 「公衆衛生に対する脅威」とは、欧州議会及び理事会の規則(EU) 2016/399 の第 2 条第 21 号に定義する公衆衛生に対する脅威のことを意味する。

第 4 条 技術アーキテクチャ及び SIS の運営方法

1. SIS は、以下によって構成される：
   (a) 以下によって構成される中央システム（中央 SIS）：
      (i) データベース（「SIS データベース」）を含み、かつ、バックアップ CS-SIS を含め、技術支援機能（「CS-SIS」）；
      (ii) 統一的な国内インタフェイス（「NI-SIS」）；
   (b) 少なくとも 1 つの国内バックアップ N.SIS または共有バックアップ N.SIS を含め、中央 SIS と通信する国内データシステムによって構成される各構成国の国内システム（「N.SIS」）；並びに、
   (c) SIS データ専用の暗号化された仮想ネットワーク及び第 7 条第 2 項に示す SIRENE 事務局間のデータ交換を提供する CS-SIS、バックアップ CS-SIS 及び NI-SIS の間の通信インフラ（「通信インフラ」）。

   (b)に示す N.SIS は、SIS データベースの完全な複製物または部分的な複製物を含むデータファイル（「国内複製物」）を含め得る。複数の構成国は、それらの構成国の N.SIS 中の 1 つの中に、それらの構成国によって共同して利用され得る共有複製物を構築し得る。そのような共有複製物は、それらそれぞれの構成国の国内複製物として判断される。

   (b)に示す共有バックアップ N.SIS は、複数の構成国によって共同して利用され得る。そのような場合、その共有バックアップ N.SIS は、それらそれぞれの構成国のバックアップ N.SIS として判断される。N.SIS 及びそのバックアップは、エンドユーザに対する途切れることのない可用性を確保するため、同時に使用され得る。

   共同して利用される共有複製物または共有バックアップ N.SIS の構築を予定する構成国は、書面により、それらの構成国それぞれの職責に合意する。それらの構成国は、欧州委員会に対し、その合意を通知する。

   通信インフラは、SIS の途切れることのない可用性を確保することを支援し、その確保に貢献する。通信インフラは、CS-SIS とバックアップ CS-SIS との間の接続のための冗長性があり、かつ、区分された経路を含めるものとし、また、個々の SIS 国内ネットワークアクセスポイントと、CS-SIS 及びバックアップ CS-SIS との間の接続のための冗長性があり、かつ、区分された経路も含める。
2. 構成国は、それらの構成国自身の N.SIS を介して、SIS データを入れ、アップデートし、そして、検索する。部分的もしくは完全な国内複製物または部分的もしくは完全な共有複製物を使用する構成国は、それら個々の構成国の領土内における自動化された検索を実施する目的のために、当該複製物を利用できるようにする。部分的な国内複製物または共有複製物は、少なくとも、第 20 条第 3 項の(a)ないし(v)に列挙するデータを収録する。共有複製物の場合を除き、別の構成国の N.SIS のデータファイルを検索してはならない。
3. CS-SIS は、技術的な監視機能及び管理機能を遂行し、かつ、当該システムの不具合の場合において主 CS-SIS の全ての機能を確保できるバックアップ CS-SIS をもつ。CS-SIS 及びバックアップ CS-SIS は、eu-LISA の 2 つの技術サイトに所在する。

4. eu-LISA は、CS-SIS の不具合の場合における SIS の運用を確保する能力をバックアップ CS-SIS が維持することを条件として、CS-SIS 及びバックアップ CS-SIS を同時運用することにより、または、システムまたはそのコンポーネントの二重化により、SIS の途切れることのない可用性を強化するための技術ソリューションを実装する。規則(EU) 2018/1726 の第 10 条に定める手続要件に拘らず、eu-LISA は、遅くとも 2019 年 12 月 28 日までに、独立の影響評価及び費用対効果分析を含め、技術ソリューションのオプションに関する調査研究を準備する。
5. 例外的な状況の下においてそれが必要なときは、eu-LISA は、一時的に、SIS データベースの追加複製物を開発できる。
6. CS-SIS は、SIS データベース内の検索を含め、SIS データの入力及び処理のために必要なサービスを提供する。国内複製物または共有複製物を使用する構成国のために、CS-SIS は:
   (a) 国内複製物のためのオンラインのアップデートを提供し;
   (b) 国内複製物と SIS データベースとの間の同期化及び一貫性を確保し;かつ、
   (c) 国内複製物の初期化及び復旧のための業務を提供する。
7. CS-SIS は、途切れることのない可用性を提供する。

第 5 条 費用

1. 中央 SIS 及び通信インフラの運営管理、維持管理、並びに、更なる開発の費用は、欧州連合の一般予算の負担とする。それらの費用は、第 4 条第 6 項に示すサービスの提供を確保するため、CS-SIS と関連して行われる作業を含める。
2. 個々の N.SIS の設置、運営、維持管理及び更なる開発の費用は、関係構成国の負担とする。

第 II 章 構成国の職責

第 6 条 国内システム

各構成国は、その構成国の N.SIS の設置、運営、維持管理及び更なる開発、並びに、NI-SIS とその構成国の N.SIS との接続について職責を負う。

各構成国は、エンドユーザに対する SIS データの途切れることのない可用性を確保することについて職責を負う。

各構成国は、その構成国の N.SIS を介して、その構成国の警報を送信する。

第 7 条 N.SIS 事務局及び SIRENE 事務局

1. 各構成国は、その構成国の N.SIS について中心的な職責を負う機関（N.SIS 事務局）を指定する。

   この機関は、N.SIS の円滑な運営及び安全性について職責を負い、職務権限を有する機関の SIS へのアクセスを確保し、かつ、この規則の遵守を確保するために必要となる措置を講ずる。その機関は、SIS の全ての機能がエンドユーザに対して適切に利用できるようにされることを確保することについて職責を負う。

2. 各構成国は、1 日 24 時間、週 7 日間業務遂行し、かつ、SIRENE マニュアルに従い、全ての補足情報の交換及び可用性を確保する国内機関（SIRENE 事務局）を指定する。各 SIRENE 事務局は、警報と関連する補足情報を交換するため、及び、個人または対象物に関する警報が SIS の中に入れられ、かつ、該当ありによってその個人または対象物が発見された場合において執られることが要求される行動を容易にするため、その SIRENE 事務局の構成国の連絡部局としての業務を提供する。

補足情報の要請に対して、迅速に、かつ、第 8 条に定める期限内に回答可能とするため、各 SIRENE 事務局は、国内法に従い、国内データベースを含め、全ての関連国内情報及びその構成国の警報に関する全ての情報、並びに、専門家の助言への直接または間接の容易なアクセスをもつ。

SIRENE 事務局は、SIS の中に入れられた情報の品質の確認を調整する。その目的のために、SIRENE 事務局は、SIS の中で処理されたデータへのアクセスをもつ。

3. 構成国は、eu-LISA に対し、その構成国の N.SIS 事務局及びその構成国の SINERE 事務局の詳細情報を提供する。eu-LISA は、第 56 条第 7 項に示すリストと共に、N.SIS 事務局及び SIRENE 事務局のリストを公表する。

第 8 条 補足情報の交換

1. 補足情報は、SIRENE マニュアルの条項に従い、かつ、通信インフラを使用して、交換される。構成国は、補足条項の継続的な可用性、及び、適時かつ効果的な交換を確保するために必要となる技術資源及び人的資源を提供する。通信インフラが利用できない場合、構成国は、補足情報を交換するために、別の十分に安全な技術的手段を利用する。十分に安全な技術的手段のリストは、SIRENE マニュアルの中で定められる。
2. 補足情報は、発行構成国から別の利用に関する同意が事前に獲得されている場合を除き、第 64 条に従って送信された目的のためにのみ、利用される。
3. SIRENE 事務局は、とりわけ、可能な限り速やかに、ただし、その要請を受けた時から 12 時間以内に、補足情報を求める要請に回答することによって、迅速かつ効率的な態様により、その職務を実施する。テロリスト行為に関する警報、身柄引渡しまたは引渡しのための逮捕の目的のために手配された者の関する警報の場合、及び、第 32 条第 1 項(c)に示す児童に関する警報の場合、SIRENE 事務局は、即時に行動する。

最も優先度の高い補足情報を求める要請は、SIRENE 書式の中で「URGENT」との印が付され、かつ、その緊急性の理由が示される。

4. 欧州委員会は、この規則による SIRENE 事務局の職務の細則、及び、「SIRENE マニュアル」と題するマニュアルの方式による補足情報の交換を定めるための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 9 条 技術上及び機能上の遵守

1. 構成国の N.SIS を設置する際、各構成国は、データの迅速かつ効果的な送信のための構成国の N.SIS と中央 SIS との互換性を確保するために設けられる共通の基準、プロトコル及び技術手

順を遵守する。

2. 構成国が国内複製物を利用する場合、その構成国は、CS-SIS から提供されるサービスにより、及び、第4条第6項に示す自動的なアップデートにより、国内複製物の中に記録保存されるデータが、SIS データベースと同じであり、かつ、それと一貫性のあるものであること、及び、その構成国の国内複製物内の検索により、SIS データベース内の検索の結果と均等な検索結果を生成することを確保する。

3. エンドユーザは、彼らの職務を遂行するために必要なデータ、とりわけ、かつ、それが必要なときは、データ主体の識別を可能とし、要求された行動を執ることを可能とする全ての利用可能なデータを取得する。

4. 構成国及び eu-LISA は、第 2 項に示す国内複製物の技術上の遵守を確認するための定期的な試験を実施する。それらの試験の結果は、理事会規則(EU) No 1053/2013[1]によって構築される仕組みの一部として考慮に入れられる。

5. 欧州委員会は、本条第 1 項に示す共通の基準、プロトコル及び技術手順を定め、策定するための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 10 条 セキュリティー構成国

1. 各構成国は、その構成国の N.SIS との関係において、セキュリティ計画、継続性計画及び災害復旧計画を含め、以下のために必要となる措置を採択する:
   (a) 重要インフラ防護のための危機管理計画の作成による場合を含め、データの物理的防護;
   (b) 個人データを処理するために使用されるデータ処理施設への無権限の者のアクセスの拒否（施設アクセス管理）;
   (c) データ媒体の無権限の閲読、複製、改変または除去の防止（データ媒体管理）;
   (d) データの無権限の入力及び記録保存された個人データの無権限の調査、改変または削除の防止（記録保存管理）;
   (e) 無権限の者によるデータ通信機器を用いて行われる自動化されたデータ処理システムの使用の防止（利用者管理）;
   (f) SIS の中にあるデータの無権限の処理、及び、SIS の中で処理されたデータの無権限の改変または削除の防止（データ入力管理）;
   (g) 自動化されたデータ処理システムの利用の承認を受けた者が、個人識別子及びユニークな利用者識別子並びに機密アクセス限定モードのみにより、彼らのアクセス承認の適用範囲内にあるデータのみに対するアクセスをもつことの確保（データアクセス管理）;
   (h) SIS へのアクセスの権利またはデータ処理施設へのアクセスの権利をもつ全ての機関が、データへのアクセス、その入力、アップデート、削除及び検索の承認を受けた者の権能及び職責を記述するプロファイルを作成し、かつ、それらの者のプロファイルを、第 69 条第 1

[1] シェンゲン協定の適用を確認するための評価及び監視の仕組みを構築し、シェンゲンの評価及び実装に関する独立委員会を設置する 1998 年 9 月 16 日の執行委員会決定を廃止する 2013 年 10 月 7 日の理事会規則(EU) No 1053/2013（OJ L 295, 6.11.2013, p.27）

項に示す監督機関の要請により、遅滞なく、それらの監督機関が利用できるようにすることの確保（個人プロファイル）；

(i) データ通信機器を用いてどの組織に対して個人データが送信され得るかを確認及び確定できることの確保（通信管理）；

(j) 自動化されたデータ処理システムの中に、どの個人データが、いつ、誰によって、どの目的のために入力されたかを事後的に確認及び確定できることの確保（入力管理）；

(k) とりわけ、適切な暗号技術により、個人データを送信する間、または、データ媒体の輸送中、個人データの無権限の閲読、複製、改変または削除の防止（輸送管理）；

(l) 本項に示すセキュリティ措置の実効性の監視、及び、この規則の遵守を確保するための内部監視と関連する必要な組織上の措置を講ずること（自己監査）；

(m) 停止の場合において、インストールされたシステムが正常な運営のために復旧され得ることの確保（復旧）；並びに、

(n) SIS がその機能を正しく遂行すること、不具合が報告されること（信頼性）、SIS の中に記録保存された個人データが、システムの不具合によって危殆に瀕することがあり得ないこと（完全性）の確保。

2. 構成国は、SIRENE 事務局の施設を防護することによる場合を含め、補足情報の処理及び交換と関係するセキュリティに関し、第 1 項に示す措置と均等な措置を講ずる。

3. 構成国は、第 44 条に示す機関による SIS データの処理と関係するセキュリティに関し、本条の第 1 項に示す措置と均等な措置を講ずる。

4. 第 1 項、第 2 項及び第 3 項に示す措置は、複数の IT システムを含む国内レベルの汎用セキュリティアプローチ及び汎用セキュリティ計画の一部とすることができる。そのような場合、本条に定める要件及びそれらの要件の SIS への適用可能性は、その計画の中で明確に定められ、かつ、その計画によって確保されるものとする。

第 11 条 機密性－構成国

1. 各構成国は、その構成国の国内法に従い、SIS データ及び補足情報を扱う仕事を要求される全ての個人及び組織に対し、職業上の秘密またはそれ以外の均等な機密保持義務に関するその構成国の規定を適用する。その義務は、それらの者が職場または就業を終えた後、または、それらの組織の活動が終了した後においても、適用される。

2. SIS と関連する職務において、構成国が外部の契約者と協力する場合、その構成国は、とりわけ、安全性、機密性及びデータ保護に関し、この規則の全ての条項の遵守を確保するため、その契約者の活動を仔細に監視する。

3. 民間会社または民間団体に対して N.SIS またはその技術複製物の業務運営管理を委託してはならない。

第 12 条 国内レベルにおける履歴（ログ）の保存

1. 構成国は、検索が適法であったか否かを確認し、データ処理の適法性を監視し、自己監視し、N.SIS の適正な稼働並びにデータの完全性及び安全性を確保する目的のために、CS-SIS 内の

個人データへの全てのアクセス及びその全ての交換がその構成国の N.SIS の中に履歴（ログ）記録されることを確保する。この要件は、第 4 条第 6 項の(a)、(b)及び(c)に示す自動化された処理には適用されない。

2. 履歴（ログ）は、とりわけ、警報の履歴、データ処理活動の日時、検索の遂行のために使用されたデータ、処理されたデータの参照、並びに、職務権限を有する機関及びデータを処理する者の両者の個人識別子及びユニークな利用者識別子を示す。
3. 本条第 2 項からの特例により、第 43 条に従って指紋検査データまたは顔画像の検索が実施された場合、その履歴（ログ）は、実データの代わりに、検索を遂行するために使用されたデータの種類を示す。
4. 履歴（ログ）は、第 1 項に示す目的のためにのみ使用され、かつ、その作成から 3 年後に削除される。警報の履歴を含む履歴（ログ）は、その警報の削除の時から 3 年後に削除される。
5. 履歴（ログ）は、既に実施されている監視手続のためにそれが必要なときは、第 4 項に示す期間よりも長く保存され得る。
6. 検索が適法であるか否かを確認し、データ処理の適法性を監視し、自己監視し、及び、N.SIS の適正な稼働並びにデータの完全性及び安全性を確保することに従事する職務権限を有する国内機関は、それらの機関の職務権限の範囲内において、かつ、それらの機関の要請により、それらの機関の責務を果たす目的のために、履歴（ログ）へのアクセスをもつ。
7. 構成国が、国内法に従い、ナンバープレート自動認識システムを用いて、自動車のナンバープレートの自動化されたスキャン検索を実施する場合、構成国は、国内法に従い、その検索の履歴（ログ）を維持管理する。必要があるときは、該当ありが得られるか否かを確認するため、SIS 内の全部検索が実施され得る。全ての全部検索に対し、第 1 項ないし第 6 項が適用される。
8. 欧州委員会は、本条第 7 項に示す履歴（ログ）の内容を定めるための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 13 条 自己監視

構成国は、SIS データへのアクセスの権利のある個々の機関が、この規則の遵守のために必要な措置を講ずること、及び、それが必要なときは、監督機関と協力することを確保する。

第 14 条 職員の訓練

1. SIS の中に記録保存されたデータを処理することの承認を受ける前に、かつ、SIS データへのアクセスが与えられた後は定期的に、SIS へのアクセスの権利をもつ機関の職員は、データのセキュリティに関し、データ保護を含め、基本的な権利に関し、並びに、SIRENE マニュアルに定めるデータ処理のための規則及び手続に関し、適切な訓練を受ける。その職員は、第 73 条に定める制裁を含め、犯罪行為及び制裁に関する関連条項の説明を受ける。
2. 構成国は、エンドユーザ及び SIRENE 事務局の職員に対する訓練を含む国内 SIS 訓練計画をもつ。

   その訓練計画は、他の関連領域の訓練を含む国内レベルの一般訓練の一部とし得る。
3. SIRENE 事務局間の協力を拡大するため、少なくとも 1 年に 1 回、欧州連合レベルで、共通の

訓練コースが組織される。

第 III 章 eu-LISA の職責

第 15 条 業務運営管理

1. eu-LISA は、中央 SIS の業務運営管理について職責を負う。eu-LISA は、構成国と協力し、費用対効果分析に従い、常に、利用可能な最善の技術が中央 SIS のために使用されることを確保する。
2. eu-LISA は、通信インフラと関連する以下の職務についても職責を負う:
   (a) 監視;
   (b) セキュリティ;
   (c) 構成国とプロバイダとの間の関係の調整;
   (d) 予算の実行と関連する職務;
   (e) 調達及び更新;並びに、
   (f) 契約上の事項。
3. eu-LISA は、SIRENE 事務局、及び、SIRENE 事務局間の通信と関連する以下の職務についても職責を負う:
   (a) 試験活動の調整、運営管理及び支援;
   (b) SIRENE 事務局間の補足情報の交換及び通信インフラの技術仕様の維持管理及び改訂;並びに、
   (c) SIS、及び、SIRENE 事務局間の補足情報の交換の両者に対してそれが影響を及ぼす場合、技術の変化の影響の管理。
4. eu-LISA は、CS-SIS の中にあるデータの品質の確認を実施するための仕組み及び手続を開発及び維持管理する。eu-LISA は、それに関し、構成国に対し、定期的に報告書を提供する。

   eu-LISA は、欧州委員会に対し、直面する問題及び関係する構成国を包摂する定期報告書を提出する。

   欧州委員会は、欧州議会及び理事会に対し、直面するデータの品質上の問題に関する定期報告書を提出する。
5. eu-LISA は、SIS の技術上の利用に関する訓練及び SIS データの品質を向上させるための措置に関する訓練の提供と関連する職務も遂行する。
6. 中央 SIS の業務運営管理は、この規則に従い、1 日 24 時間、週 7 日間、中央 SIS の稼働を維持するために必要となる全ての職務、とりわけ、システムの円滑な作動のために必要となる保守管理作業及び技術開発によって構成される。それらの職務は、第 9 条に定める技術上及び機能上の遵守の要件に従って中央 SIS 及び N.SIS が運用されることを確保する中央 SIS 及び N.SIS の試験活動の調整、維持管理及び支援も含める。
7. 欧州委員会は、通信インフラの技術上の要求事項を定めるための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 16 条　セキュリティーeu-LISA

1. eu-LISA は、以下のために、中央 SIS 及び通信インフラに関し、セキュリティ計画、継続性計画及び災害復旧計画を含め、必要な措置を採択する:
   (a) 重要インフラの防護のための危機管理計画の作成による場合を含め、データの物理的な防護;
   (b) 個人データを処理するために使用されるデータ処理施設への無権限の者のアクセスの拒否（施設アクセス管理）;
   (c) データ媒体の無権限の閲読、複製、改変または除去の防止（データ媒体管理）;
   (d) データの無権限の入力及び記録保存された個人データの無権限の調査、改変または削除の防止（記録保存管理）;
   (e) 無権限の者によるデータ通信機器を用いて行われる自動化されたデータ処理システムの使用の防止（利用者管理）;
   (f) SIS の中にあるデータの無権限の処理、及び、SIS の中で処理されたデータの無権限の改変または削除の防止（データ入力管理）;
   (g) 自動化されたデータ処理システムの利用の承認を受けた者が、個人識別子及びユニークな利用者識別子並びに機密アクセス限定モードのみにより、彼らのアクセス承認の適用範囲内にあるデータのみに対するアクセスをもつことの確保（データアクセス管理）;
   (h) データまたはデータ処理施設へのアクセスの承認を受けた者の権能及び職責を記述するプロファイルを作成し、かつ、それらのプロファイルを、要請により、遅滞なく、欧州データ保護監督官が利用できるようにすることの確保（個人プロファイル）;
   (i) データ通信機器を用いてどの組織に対して個人データが送信され得るかを確認及び確定できることの確保（通信管理）;
   (j) 自動化されたデータ処理システムの中に、どの個人データが、いつ、誰によって、どの目的のために入力されたかを事後的に確認及び確定できることの確保（入力管理）;
   (k) とりわけ、適切な暗号技術により、個人データを送信する間、または、データ媒体の輸送中、個人データの無権限の閲読、複製、改変または削除の防止（輸送管理）;
   (l) 本項に示すセキュリティ措置の実効性の監視、及び、この規則の遵守を確保するための内部監視と関連する必要な組織上の措置を講ずること（自己監査）;
   (m) 停止の場合において、インストールされたシステムが正常な運営のために復旧され得ることの確保（復旧）;
   (n) SIS がその機能を正しく遂行すること、不具合が報告されること（信頼性）、SIS の中に記録保存された個人データが、システムの不具合によって危殆に瀕することがあり得ないこと（完全性）の確保;並びに、
   (o) SIS の技術サイトのセキュリティの確保。
2. eu-LISA は、通信インフラを介する補足情報の処理及び交換と関係するセキュリティに関し、第 1 項に示す措置と均等な措置を講ずる。

第 17 条　機密性－eu-LISA

1. 職員規則の第 17 条を妨げることなく、eu-LISA は、SIS データを扱う仕事を要求される全ての eu-LISA 職員に対し、この規則の第 11 条に定めるものと同等の基準による、職業上の秘密またはそれ以外の均等な機密保持義務に関する規定を適用する。その義務は、それらの者が職場または就業を終えた後、または、それらの活動が終了した後においても、適用される。
2. eu-LISA は、通信インフラを介する補足情報の処理及び交換と関係する機密性に関し、第 1 項に示す措置と均等な措置を講ずる。
3. SIS と関連する職務において、eu-LISA が外部の契約者と協力する場合、eu-LISA は、とりわけ、安全性、機密性及びデータ保護に関し、この規則の全ての条項の遵守を確保するため、その契約者の活動を仔細に監視する。
4. 民間会社または民間団体に対して CS-SIS の業務運営管理を委託してはならない。

第 18 条　中央レベルにおける履歴（ログ）の保存

1. eu-LISA は、第 12 条第 1 項に示す目的のために、CS-SIS 内の個人データへの全てのアクセス及びその全ての交換が履歴（ログ）記録されることを確保する。
2. 履歴（ログ）は、とりわけ、警報の履歴、データ処理活動の日時、検索の遂行のために使用されたデータ、処理されたデータの参照、並びに、データを処理する職務権限を有する機関の個人識別子及びユニークな利用者識別子を示す。
3. 本条第 2 項からの特例により、第 43 条に従って指紋検査データまたは顔画像の検索が実施された場合、その履歴（ログ）は、実データの代わりに、検索を遂行するために使用されたデータの種類を示す。
4. 履歴（ログ）は、第 1 項に示す目的のためにのみ使用され、かつ、その作成から 3 年後に削除される。警報の履歴を含む履歴（ログ）は、その警報の削除の時から 3 年後に削除される。
5. 履歴（ログ）は、既に実施されている監視手続のためにそれが必要なときは、第 4 項に示す期間よりも長く保存され得る。
6. 自己監視の目的並びに CS-SIS の適正な稼働、データの完全性及び安全性を確保する目的のために、eu-LISA は、その職務権限の範囲内において、その履歴（ログ）へのアクセスをもつ。

   欧州データ保護監督官は、その職務権限の範囲内において、かつ、その職務を満たす目的のために、要請により、それらの履歴（ログ）へのアクセスをもつ。

第 IV 章　公衆に対する情報提供

第 19 条　SIS 情報提供キャンペーン

この規則の適用開始の際、欧州委員会は、監督機関及び欧州データ保護監督官と協力して、SIS の目的、SIS の中に記録保存されるデータ、SIS へのアクセスをもつ機関、及び、データ主体の権利に関する情報を公衆に対して提供するキャンペーンを実施する。欧州委員会は、監督機関及び欧州データ保護監督官と協力して、そのようなキャンペーンを定期的に反復実施する。欧

州委員会は、SIS に関する全ての関連情報を提供し、公衆が利用可能な Web サイトを維持管理する。構成国は、その構成国の監督機関と協力して、その構成国の市民及び居住者に対して SIS 一般に関する情報を提供するために必要となる政策を立案及び実装する。

第 V 章　データ及びフラグの類型

第 20 条　データの類型

1. 第 8 条第 1 項または追加データの記録保存を定めるこの規則の条項を妨げることなく、SIS は、各構成国から供給され、第 26 条、第 32 条、第 34 条、第 36 条、第 38 条及び第 40 条に定める目的のために必要な類型のデータに限り、収録する。
2. データの類型は、以下のとおりである：
   (a) 当該の者に関する警報が入れらた者に関する情報；
   (b) 第 26 条、第 32 条、第 34 条、第 36 条及び第 38 条に示す対象物に関する情報。
3. 個人に関する情報を含む SIS 内の警報は、以下のデータのみを含める：
   (a) 姓；
   (b) 名；
   (c) 出生時の名；
   (d) 過去に使用していた名及び別名；
   (e) 変更されない、特定の、客観的で物理的な特徴；
   (f) 出生の場所；
   (g) 出生の日；
   (h) 性；
   (i) 保有している国籍；
   (j) 関係する者が：
      (i) 武装しているか否か；
      (ii) 暴力的であるか否か；
      (iii) 逃走または逃亡したか否か；
      (iv) 自殺のリスクを示しているか否か；
      (v) 公衆衛生に対する脅威を示しているか否か；
      (vi) 指令(EU) 2017/541 の第 3 条ないし第 14 条に示す活動に関与しているか否か；
   (k) その警報の根拠；
   (l) その警報を作成した機関；
   (m) 警報を発生させた決定の参照；
   (n) 該当ありの場合において行われるべき行動；
   (o) 第 63 条による別の警報とのリンク；
   (p) 侵害行為の種類；
   (q) 国内登録簿中のその者の登録番号；
   (r) 第 32 条第 1 項に示す警報に関し、その字形の種類の類型；
   (s) その者の身分証明書の類型；

(t) その者の身分証明書の発行国;
(u) その者の身分証明書の番号;
(v) その者の身分証明書の発行日;
(w) 写真及び顔画像;
(x) 第 42 条第 3 項に従い、関連する DNA プロファイル;
(y) 指紋検査データ;
(z) 可能であればカラーで、その身分証明書の複製物。

4. 欧州委員会は、本条第 2 項及び第 3 項に示すデータの入力、アップデート、削除及び検索のために必要な技術規則、並びに、本条第 5 項に示す共通基準を定め、策定するための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。
5. CS-SIS 内、国内複製物または共有複製物内、及び、第 56 条第 2 項に基づいて作成された技術複製物内の検索に関する技術規則は、同じものとする。

第 21 条 比例性

1. 警報を入れる前に、及び、警報の有効期限を延長する際、構成国は、その案件が、SIS 内の警報を保証するために十分に適切であり、関連性があり、かつ、重要であるか否かを判断する。
2. ある個人または対象物が、テロリスト行為と関連する警報に基づいて求められる場合、その案件は、SIS 内の警報を保証するために十分に適切であり、関連性があり、かつ、重要であると判断される。公共の安全または国家安全保障を理由として、構成国は、それが公的調査または法律上の調査、捜査または手続の妨げとなり得るおそれがある場合、例外として、SIS の中に警報を入れることを控えることができる。

第 22 条 警報の入力に関する要件

1. 第 40 条に示す状況の下にある場合を除き、SIS の中に警報を入れるために必要なミニマムのデータのセットは、第 20 条第 3 項の(a)、(g)、(k)及び(n)に示すデータである。それが利用可能なときは、同項に示すその他のデータも SIS の中に入れられる。
2. この規則の第 20 条第 3 項の(e)に示すデータは、関係する個人の識別のために厳格に必要な場合に限り、入れられる。そのようなデータが入れられる場合、構成国は、規則(EU) 2016/680 の第 10 条が遵守されることを確保する。

第 23 条 警報の互換性

1. 警報を入れる前に、構成国は、関係する個人または対象物が既に SIS の中の警報の対象となっているか否かを確認する。その者が既に警報の対象者となっているか否かを確認するため、そのようなデータが利用可能であるときは、指紋検査データの確認も実施される。
2. 構成国毎に、個人毎及び対象物毎に、1 つの警報のみが SIS の中に入れられる。それが必要な場合、第 3 項に従い、別の構成国によって、同一の個人または同一の対象物に関し、新たな警報が入れられ得る。

3. ある個人または対象物が既に SIS 内の警報の対象となっている場合、新たな警報を入れることを望む構成国は、それらの警報の間に互換性のない状態が存在しないことを確認する。互換性のない状態が存在しない場合、その構成国は、新たな警報を入れることができる。その警報に互換性がない場合、関係する構成国の SIRENE 事務局は、合意に達するため、補足情報の交換を介して、相互に協議する。警報の互換性に関する規則は、SIRENE マニュアルの中で定められる。重要な国家的利益が問題となる場合、構成国間の協議を経た上で、互換性の規則に依らないこととし得る。
4. 同一の個人または対象物に関して複数の警報の該当ありとなる場合、執行構成国は、SIRENE マニュアルの中で定められる警報の優先性の規則を尊重する。

ある者が、異なる構成国によって入れられた複数の警報に服する場合、第 26 条に従って入れられた逮捕のための警報は、第 25 条に従い、優先的なものとして執行される。

第 24 条 フラグに関する総則的な条項

1. ある構成国が、第 26 条、第 32 条または第 36 条に従って入れられた警報を有効とすることがその構成国の国内法、国際的な義務または重要な国内利益に適合しないと判断する場合、その構成国は、その警報に基づき執られるべき行動がその構成国の領土内においては執られない効果を発生させるためのフラグをその警報に付加することを要求できる。そのフラグは、発行構成国の SIRENE 事務局によって付加される。
2. 第 26 条に従って入れられた警報にフラグが付加されることを構成国が要求できるようにするため、全ての構成国は、補足情報の交換を介して、自動的に、その類型の新たな警報の通知を受ける。
3. とりわけ、緊急かつ重大な場合において、発行構成国が行動を執ることを要請するときは、執行構成国は、付されたフラグが撤回されることを要望できるようにするか否かを検討する。その執行構成国がそのようにできる場合、その執行構成国は、執られるべき行動が直ちに実施され得ることを確保するために必要となる手立てを講ずる。

第 25 条 身柄引渡しの目的のための逮捕と関連するフラグ

1. 枠組み決定 2002/584/JHA が適用される場合において、国内法に基づき欧州逮捕令状の執行について職務権限を有する法務当局が不執行のための根拠に基づいてその執行を拒絶し、かつ、フラグの付加が要請されたときは、構成国は、発行構成国に対し、フォローアップとして、身柄引渡しの目的のための逮捕に関する警報に逮捕を妨げるフラグを付加することを要請する。

構成国は、その構成国の職務権限を有する法務当局が、身柄拘束の過程の間に、その警報の対象者を解放したときにおいても、その警報にフラグを付加することを要請できる。
2. ただし、欧州逮捕令状の執行が拒否されることが明らかであるときは、一般的な指示に基づき、または、個別の事件において、職務権限を有する法務当局の要望により、国内法に基づき、構成国は、その発行構成国に対し、身柄引渡しの目的のための逮捕に関する警報にフラグを付加することを要請することもできる。

第 VI 章　身柄引渡しまたは引渡しの目的のための逮捕の手配のある者に関する警報

第 26 条　警報を入れる目的及び条件

1. 欧州逮捕令状に基づく身柄引渡しの目的のための逮捕の手配のある個人に関する警報、または、引渡しの目的のための逮捕の手配のある個人に関する警報は、発行構成国の職務権限を有する法務当局の要請により、入れられる。
2. 身柄引渡しの目的のための逮捕に関する警報は、逮捕令状に基づく個人の身柄引渡しの目的のために、諸条約を基礎として欧州連合と第三国との間で締結され、そのような逮捕令状の SIS を介する送付を定める協定に従い、発付された逮捕令状に基づいても入れられる。
3. この規則内にある枠組み決定 2002/584/JHA の条項への参照は、逮捕令状に基づく個人の身柄引渡しの目的のために、諸条約を基礎として欧州連合と第三国との間で締結され、そのような逮捕令状の SIS を介する送付を定める協定の対応する条項を含めるものとして解釈されるものとする。
4. 現在進行中の業務遂行の場合、発行構成国は、本条に従って入れられた逮捕に関する既存の警報を、一時的に、その業務遂行に関与する構成国内のエンドユーザから検索できないようにすることができる。そのような場合、その警報は、SIRENE 事務局に対してのみアクセス可能とする。構成国は、以下の場合に限り、警報を利用できないようにする:
   (a) 他の手段によっては業務遂行の目的を達成することができず;
   (b) 発行構成国の職務権限を有する法務当局から事前の承認が与えられており;かつ、
   (c) その業務遂行に関与する全ての構成国が補足条項の交換を介して通知を受けている場合。

   第 1 副項に定める機能は、48 時間を超過しない時間内に限り、使用される。ただし、業務遂行上必要なときは、更に 48 時間まで延長され得る。構成国は、その警報に関してこの機能が使用された警報の数の統計を保存する。
5. 第 38 条第 2 項の(a)、(b)、(c)、(e)、(g)、(h)、(j)及び(k)に示す対象物が、本条の第 1 項または第 2 項による警報の対象者である個人と関係しているとの徴証が存在する場合、その者を発見するためにそれらの対象物に関する警報を入れることができる。そのような場合、その個人に関する警報及びその対象物に関する警報は、第 63 条に従ってリンクされる。
6. 欧州委員会は、本条第 5 項に示すデータの入力、アップデート、削除及び検索のために必要となる規則を定め、策定するための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 27 条　身柄引渡しの目的のための逮捕の手配のある者に関する追加データ

1. ある者が、欧州逮捕令状に基づき、身柄引渡しの目的のために逮捕の手配のある者である場合、その発行構成国は、欧州逮捕令状の原本の複製物を SIS の中に入れる。

   構成国は、身柄引渡しの目的のための逮捕に関する 1 つの警報の中に、複数の欧州逮捕令状の複製物を入れることができる。
2. 発行構成国は、欧州連合の機関の 1 または複数の別の公用語による欧州逮捕令状の翻訳文の複製物を入れることができる。

第 28 条　身柄引渡しの目的のための逮捕の手配のある者に関する補足情報

身柄引渡しのための体法に関する警報の発行構成国は、別の構成国に対し、補足情報の交換を介して、枠組み決定 2002/584/JHA の第 8 条第 1 項に示す情報を送付する。

第 29 条　引渡しの目的のための逮捕の手配のある者に関する補足情報

1. 引渡しの目的のための警報の発行構成国は、補足情報の交換を介して、他の全ての構成国に対し、以下のデータを送付する:
   (a) 逮捕を求める要請を発した機関;
   (b) 逮捕令状、もしくは、それと同じ法的効力をもつ文書、または、執行可能な判決が存在するか否か;
   (c) その侵害行為の性質及び法律上の区分;
   (d) その警報が入れられた者による侵害行為の時、場所及び関与の程度を含め、その侵害行為が実行された状況の記述;
   (e) 可能な範囲内において、その侵害行為の結果;並びに、
   (f) その警報の執行にとって有用または必要な上記以外の情報。
2. 第 27 条または第 28 条に示すデータが既に提供されている場合、及び、執行構成国による警報の執行のために十分であると判断される場合、本条第 1 項に列挙するデータを送付してはならない。

第 30 条　身柄引渡しまたは引渡しの目的のための逮捕に関する警報に関して採られるべき行動の切り替え

第 24 条もしくは第 25 条に定めるフラグを立てる手続に従い、そのようにすることを求められた構成国がそのようにすることを拒否していることにより、または、引渡しの目的のための逮捕に関する警報の場合において、捜査が完了していないということにより、逮捕が行われ得ない場合、逮捕を行うことを要請した構成国は、関係する者の所在を連絡することにより、警報上で行動する。

第 31 条　身柄引渡しまたは引渡しの目的のための逮捕に関する警報に基づく行動の執行

1. 第 26 条に従って SIS の中に入れられた警報及び第 27 条に示す追加データは、枠組み決定 2002/584/JHA が適用される場合、同決定に従って発付された欧州逮捕令状と同じ効果を構成し、その効果をもつ。
2. 枠組み決定 2002/584/JHA が適用されない場合、第 26 条及び第 29 条に従って SIS の中に入れられた警報は、引渡しに関する 1957 年 12 月 13 日の欧州条約の第 16 条、または、刑事における引渡し及び共助に関する 1962 年 6 月 27 日のベネルクス条約の第 15 条に基づく一時的な逮捕の要請と同じ法的効力をもつ。

第 VII 章　失踪児童または旅行を阻止される必要のある脆弱性のある者に関する警報

第 32 条　データを入れるための目的及び条件

1. 以下の類型の者に関する警報は、発行構成国の職務権限を有する機関の要請により、SIS の中に入れられる：
   (a) 保護の下に置かれる必要のある失踪者：
      (i) 彼ら自身の保護のために；
      (ii) 公共の秩序または公共の安全に対する脅威を防止するために；
   (b) 保護の下に置かれる必要のない失踪者；
   (c) 親、家族または後見人による連れ去りの脅威に直面しており、旅行が阻止される必要性のある児童；
   (d) ある構成国の領土からの連れ去される、または、退去させられる具体的かつ明白なリスク、並びに、以下のリスクのゆえに、彼ら自身の保護のために旅行が阻止される必要性のある児童：
      (i) 人身取引の被害者となるリスク、強制婚姻もしくは女性器切除またはそれ以外の性暴力の被害者となるリスク；
      (ii) テロリスト犯罪の被害者または加担者となるリスク；
      (iii) 武装グループへ徴兵または加入させられるリスク、または、兵站の活動に加担させられるリスク；
   (e) ある構成国の領土からの連れ去される、または、退去させられる具体的かつ明白なリスク、並びに、人身取引または性暴力の被害者となるリスクのゆえに、その脆弱性があり、その年齢であり、彼ら自身の保護のために旅行が阻止される必要性のある者。
2. 第 1 項の(a)は、とりわけ、児童、及び、職務権限を有する機関による決定に従って収容されなければならない者に対して適用される。
3. 第 1 項の(c)に示す児童に関する警報は、その職務権限を有する機関が所在している構成国から違法かつ直ちに退去されられ得るという具体的かつ明白なリスクが存在する場合、親権に関する事項の管轄権をもつ構成国の法務当局を含め、職務権限を有する機関の決定により、入れらる。
4. 第 1 項の(d)及び(e)に示す者に関する警報は、法務当局を含め、職務権限を有する機関による決定により、入れられる。
5. 発行構成国は、第 53 条第 4 項に従い、本条第 1 項の(c)、(d)及び(e)に示す警報を維持する必要性を継続的に見直す。
6. 発行構成国は、以下の全てのことを確保する：
   (a) その警報と関係する者が第 1 項に示す類型のどの範囲内にあるかをその発行構成国が入れたデータが示すものであること；
   (b) 事件の種類が認知されている限り、どの種類の事件が含まれているかをその発行構成国が入れたデータが示すものであること；かつ、
   (c) 第 1 項の(c)、(d)及び(e)に従って入れられた警報との関係において、その発行構成国の SIRENE 事務局が、その警報の作成時点において任意に利用できる全ての関連情報をも

つこと。

7. 本条に基づく警報の対象者である児童が、発行構成国の国内法による成人に達する 4 か月前に、CS-SIS は、自動的に、その発行構成国に対し、警報の根拠及び執られるべき行動の両者がアップデートされなければならないこと、または、その警報が削除されなければならないことを通知する。
8. 第 38 条第 2 項の(a)、(b)、(c)、(e)、(g)、(h)及び(k)に示す対象物が、本条第 1 項による警報の対象者である個人と関係しているとの徴証が存在する場合、その者を発見するため、それらの対象物に関する警報を入れることができる。そのような場合、その個人に関する警報及びその対象物に関する警報は、第 63 条に従ってリンクされる。
9. 欧州委員会は、本条第 8 項に示すデータの入力、アップデート、削除及び検索のために必要となる規則を定め、策定するための実装行為を採択する。

それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 33 条 警報に基づく行動の執行

1. 第 32 条に示す者が所在する場合、その執行構成国の職務権限を有する機関は、第 4 項に従い、その発行構成国に対し、彼または彼女の所在を連絡する。
2. 第 32 条の(a)、(c)、(d)及び(e)に示す保護の下に置かれる必要性のある者の場合、その執行構成国は、講じられるべき措置を遅滞なく合意するため、直ちに、補足情報の交換を介して、その執行構成国自身の職務権限を有する機関及びその発行構成国の職務権限を有する機関と協議する。執行構成国の職務権限を有する機関は、国内法に従い、そのような者の旅行の継続を阻止するため、そのような者を安全な場所へ移すことができる。
3. 児童の場合、第 2 項に示す安全な場所へその児童を移すために講じられる措置またはそのための決定は、その児童の最善の利益に従って行われる。そのような決定は、直ちに行われ、かつ、関連児童保護機関としかるべく協議した上で、その児童が発見された後、遅くとも 12 時間以内に行われるものとする。
4. 職務権限を有する機関の間における通信以外の、発見され、その年齢である失踪者に関するデータの送信は、当該の者の同意に服する。ただし、職務権限を有する機関は、当該の者が失踪中であることを通報した者に対し、その失踪者が発見されたためにその警報が削除されたことを連絡する。

第 VIII 章 法務上の手続の支援が求められている者に関する警報

第 34 条 データを入れるための目的及び条件

1. 個人の居住地または住所地を連絡する目的のために、構成国は、職務権限を有する機関の要請により、以下の者に関する警報を SIS の中に入れる:
   (a) 証言者;
   (b) 刑事手続との関係において、彼らが訴追されている行為について弁明するため、法務当局に出頭した者、または、その出頭を求められている者;

(c) 刑事判決を受けるべき者、または、彼らが訴追されている行為について弁明するため、刑事手続と関係する判決以外の文書を受けるべき者;

(d) 自由剥奪刑を含む刑罰を受けるための出頭を求める召喚状を受けるべき者。

2. 第 38 条第 2 項の(a)、(b)、(c)、(e)、(g)、(h)及び(k)に示す対象物が、本条第 1 項による警報の対象者である個人と関係しているとの徴証が存在する場合、その者を発見するため、それらの対象物に関する警報を入れることができる。そのような場合、その個人に関する警報及びその対象物に関する警報は、第 63 条に従ってリンクされる。

3. 欧州委員会は、本条第 2 項に示すデータの入力、アップデート、削除及び検索のために必要となる規則を定め、策定するための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 35 条 警報に基づく行動の執行

要請された情報は、補足情報の交換を介して、発行構成国に対して送付される。

第 IX 章 慎重な検問、質問による検問及び個別の検問を要する個人に関する警報及び対象物に関する警報

第 36 条 データを入れるための目的及び条件

1. 個人に関する警報、第 38 条第 2 項の(a)、(b)、(c)、(e)、(g)、(h)、(j)、(k)及び(l)に示す対象物に関する警報、並びに、非現金の決済手段に関する警報は、発行構成国の国内法に従い、第37条第 3 項、第 4 項及び第 5 項による慎重な検問、質問による検問または個別の検問の目的のために、入れられる。

2. 慎重な検問、質問による検問または個別の検問に関する警報が入れられる際、かつ、その発行構成国から求められる情報が、第 37 条第 1 項の(a)ないし(h)に定める情報に付加されるものである場合、その発行構成国は、求められている全ての情報をその警報に付加する。その情報が、指令(EU) 2016/680 の第 10 条に示す特別類型の個人データと関連するものである場合、その警報の個別の目的のために、かつ、その警報が入れられた犯罪行為との関係において、その個人データが厳格に必要である場合に限り、その個人データを求めることができる。

3. 慎重な検問、質問による検問または個別の検問に関する警報は、犯罪行為の防止、検知、捜査または訴追、刑罰の執行、及び、公共の安全に対する脅威の防止の目的のために、以下の 1 または複数の状況の下において、これを入れることができる:

(a) 枠組み決定 2002/584/JHA の第 2 条第 1 項及び第 2 項に示す侵害行為のいずれかを実行することを意図する者、または、それを実行中の者であるとの明確な徴証が存在する場合;

(b) 枠組み決定 2002/584/JHA の第 2 条第 1 項及び第 2 項に示す侵害行為のいずれかの有罪判決を受けた者に関する拘禁刑または拘禁命令の執行のため、第 37 条第 1 項に示す情報が必要な場合;

(c) とりわけ、過去の犯罪行為を基礎として、ある者の全体評価の結果が、将来において、枠組み決定 2002/584/JHA の第 2 条第 1 項及び第 2 項に示す侵害行為を実行するおそれがあ

ると信ずる根拠を与える場合。

4. 加えて、関係する者によって示される重大な脅威または国内の安全もしくは国家安全保障に対するその他の重大な脅威を防止するため、第 37 条第 1 項に示す情報が必要であるとの具体的な徴証が存在する場合、国家安全保障について職責を負う機関の要請に応じて、国内法に従い、慎重な検問、質問による検問または個別の検問に関する警報を入れることができる。本項に従って警報を入れた構成国は、他の構成国に対し、そのような警報を通知する。各構成国は、その情報がどの機関に対して転送されるべきかを決定する。その情報は、SIRENE 事務局を介して転送される。

5. 第 38 条第 2 項の(a)、(b)、(c)、(e)、(g)、(h)、(j)、(k)及び(l)に示す対象物と関係しているとの明確な徴証が存在する場合、または、非現金の決済手段が本条第 3 項に示す重大犯罪もしくは本条第 4 項に示す重大犯罪と関係するものである場合、本条第 3 項及び本条第 4 項に従い、その警報及びリンクの中にそれらの対象物に関する警報を入れることができる。

6. 欧州委員会は、本条第 5 項に示すデータ及び本条第 2 項に示す追加情報の入力、アップデート、削除及び検索のために必要となる規則を定め、策定するための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 37 条 警報に基づく行動の執行

1. 慎重な検問、質問による検問または個別の検問の目的のために、執行構成国は、以下の情報の全部または一部を収集し、それを発行構成国に対して送付する：
   (a) 警報の対象者である者が発見されたという事実、第 38 条第 2 項の(a)、(b)、(c)、(e)、(g)、(h)、(j)、(k)及び(l)に示す対象物、または、警報の対象物である非現金の決済手段が発見されたという事実；
   (b) その検問の場所、時及び理由；
   (c) 旅行行程及び到着地；
   (d) 警報の対象物を所持する者、または、自動車、船舶もしくは航空機の乗員、または、白地の公文書または既発行身分証明書の保有者を伴う者であって、その警報の対象物と関係すると合理的に予測され得る者；
   (e) 警報の対象物である白地の公文書または既発行身分証明書を使用する者の、明らかにされた識別名及び身上関係の記述；
   (f) 使用された第 38 条第 2 項の(a)、(b)、(c)、(e)、(g)、(h)、(j)、(k)及び(l)に示す対象物、または、使用された非現金の決済手段；
   (g) 旅行文書を含め、運搬された対象物；
   (h) その個人、第 38 条第 2 項の(a)、(b)、(c)、(e)、(g)、(h)、(j)、(k)及び(l)に示す対象物または非現金の決済手段が発見された状況；
   (i) 第 36 条第 2 項により発行構成国から求められている上記以外の情報。

   本項第 1 副項の(i)に示す情報が指令(EU) 2016/680 の第 10 条に示す特別類型の個人データであるときは、その個人データは、同条に定める条件に従い、かつ、その個人データが同じ目的のために処理される別の個人データを補完するものである場合に限り、処理される。

2. 執行構成国は、補足情報の交換を介して、第 1 項に示す情報を送付する。

3. 慎重な検問は、執行構成国の職務権限を有する国内機関によって実施される通常業務活動の間に可能な範囲内にある第 1 項に示す情報の慎重な収集によって構成される。その情報の収集は、検問の慎重性を危険に晒してはならず、かつ、いかなる態様によっても警報の対象者がその警報が存在することに気づかないようなものとする。
4. 質問による検問は、第 36 条第 2 項に従い、発行構成国によって警報に付加された情報または個別の質問を基礎とする場合を含め、その個人に対する質問によって構成される。その質問は、執行構成国の国内法に従って実施される。
5. 個別の検問の間、個人、自動車、船舶、航空機、コンテナ及び運搬された対象物は、第 36 条に示す目的のために捜索され得る。捜索は、執行構成国の国内法に従って実施される。
6. 個別の検問が執行構成国の国内法によって認められない場合、個別の検問は、当該構成国における質問による検問によって置き換えられる。質問による検問が執行構成国の国内法によって認められない場合、質問による検問は、当該構成国における慎重な検問によって置き換えられる。指令 2013/48/EU が適用される場合、構成国は、同指令に定める条件に従い、弁護士へのアクセスをもつための容疑者及び被訴追者の権利が尊重されることを確保する。
7. 第 6 項は、第 36 条第 2 項に基づいて求められるエンドユーザの情報を利用できるようにすべき構成国の義務を妨げない。

第 X 章 刑事手続における差押えまたは証拠としての使用のための対象物に関する警報

第 38 条 データを入れるための目的及び条件

1. 構成国は、刑事手続における差押えまたは証拠としての使用の目的のために求められる対象物に関する警報を SIS の中に入れる。
2. 警報は、以下の容易に識別可能な対象物の類型に基づき、入れられる：
   (a) 原動機の別に拘らず、自動車;
   (b) 積載重量が 750 キログラムを超過するトレーラー;
   (c) 移動住宅;
   (d) 産業機器;
   (e) 船舶;
   (f) 船舶用エンジン;
   (g) コンテナ;
   (h) 航空機;
   (i) 航空機用エンジン;
   (j) 武器;
   (k) 盗難、不正流用、紛失した白地の公文書、または、そのような文書であると主張されているが、偽造である文書;
   (l) 旅券、身分証明カード、居住許可証、旅行文書及び運転免許証のような、盗難、不正流用、紛失した既発行身分証明書、または、そのような文書であると主張されているが、偽造である文書;
   (m) 盗難、不正流用、紛失した白地の公文書、または、そのような文書であると主張されている

が、偽造である自動車登録証明書及び自動車ナンバープレート;

(n) 紙幣（登録紙幣）及び偽造紙幣;

(o) 情報技術のアイテム;

(p) 自動車の識別可能な構成部品;

(q) 産業機器の識別可能な構成部品;

(r) 第 3 項に従って定められる上記以外の高価な識別可能対象物。

(k)、(l)及び(m)に示す文書に関し、発行構成国は、そのような文書が盗難、不正流用、紛失、無効または偽造であるか否かを指示できる。

3. 欧州委員会は、本条第 2 項の(o)、(p)、(q)及び(r)の下にある対象物の新たな下位類型を定めることによってこの規則を改正するため、第 75 条により委任される行為を採択する権限を与えられる。

4. 欧州委員会は、本条第 2 項に示すデータの入力、アップデート、削除及び検索のために必要となる技術規則を定め、策定するための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 39 条 警報に基づく行動の執行

1. 検索が、発見された対象物に関する警報を注視するものである場合、職務権限を有する機関は、その機関の構成国の国内法に従い、その対象物を差押え、かつ、講じられるべき措置に関して合意するため、発行構成国の機関と連絡をとる。その目的のために、この規則に従い、個人データも送付され得る。

2. 第 1 項に示す情報は、補足情報の交換を介して送付される。

3. 執行構成国は、国内法に従い、要請された措置を講ずる。

第 XI 章 国内法に基づく識別の目的のための未認知手配者に関する警報

第 40 条 国内法に基づく識別の目的のための未認知手配者に関する警報

構成国は、指紋検査データのみを含む未認知手配者に関する警報を SIS の中に入れることができる。それらの指紋検査データは、現在捜査中のテロリスト犯罪またはそれ以外の重大犯罪の現場において発見された完全なセットまたは不完全なセットの指紋または掌紋である。それらの指紋検査データは、その指紋検査データがその侵害行為の加害者に帰属するとの非常に高度の蓋然性が確認され得る場合に限り、SIS の中に入れられる。

発行構成国の職務権限を有する機関が、関連する他の国民のデータを基礎として容疑者の識別名を確認できない場合、第 1 副項に示す指紋検査データは、そのような者を識別する目的のために、「未認知手配者」として、その類型の警報の中にのみ入れられ得る。

第 41 条 警報に基づく行動の執行

第 40 条により入れられたデータの該当ありがある場合、その者の識別名は、SIS 内のデータが

当該の者に属することの専門家の確認と共に、国内法に従って確認される。執行構成国は、その事件の適時の捜査を容易にするため、発行構成国に対し、補足情報の交換を介して、その者の識別名及び所在に関する情報を送付する。

第 XII 章　生体データに関する特別規定

第 42 条　写真、顔画像、指紋検査データ及び DNA プロファイルを入れることに関する特別規定

1. データのミニマムの品質基準及び技術仕様を満たす第20条第3項の(w)及び(y)に示す写真、顔画像及び指紋検査データに限り、SIS の中に入れられる。そのようなデータが入れられる前に、データのミニマムの品質基準及び技術仕様に適合するか否かを確認するため、品質の確認が実施される。
2. SIS に入れられる指紋検査データは、1 個ないし 10 個の平置き指紋及び 1 個ないし 10 個の回転指紋によって構成される。そのデータは、2 個までの掌紋も含め得る。
3. DNA プロファイルは、第 32 条第 1 項の(a)に定める状況下にある場合に限り、かつ、データのミニマムの品質基準及び技術仕様に適合するか否かを確認するための品質確認の後に限り、かつ、写真、顔画像または指紋検査データが利用できない場合、もしくは、識別のために適切ではない場合に限り、警報の中に付加され得る。警報の対象者の直接の親、子、兄弟姉妹の DNA プロファイルは、それらの者が明示の同意を与えることを条件として、その警報の中に付加され得る。DNA プロファイルが警報の中に付加される場合、当該プロファイルは、失踪者の識別のための厳格に必要なミニマムの情報を含める。
4. データのミニマムの品質基準及び技術仕様は、本条第 1 項及び第 3 項に示す生体データの記録保存に関する本条第 5 項に従って策定される。それらのデータのミニマムの品質基準及び技術仕様は、第 43 条第 1 項に従って個人の同一性を確認するためのデータを使用するため、及び、第 43 条第 2 項ないし第 4 項に従って個人を識別するためのデータを使用するために要求される品質のレベルを定める。
5. 欧州委員会は、本条第 1 項、第 3 項及び第 4 項に示すデータのミニマムの品質基準及び技術仕様を定めるための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 43 条　写真、顔画像、指紋検査データ及び DNA プロファイルの確認または検索に関する特別規定

1. 写真、顔画像、指紋検査データ及び DNA プロファイルが SIS 内の警報の中で利用可能な場合、そのような写真、顔画像、指紋検査データ及び DNA プロファイルは、SIS の中で行われた符号の検索の結果として発見された者の同一性を確認するために使用される。
2. 指紋検査データは、全ての場合において、個人を識別するために検索され得る。ただし、指紋検査データは、他の手段によっては個人の同一性が確認され得ない場合において、個人の識別のために検索される。その目的のために、中央 SIS は、自動指紋識別システム（AFIS）を含める。
3. それらのセットの紋が侵害行為の実行者に属するという高度の蓋然性が確認され得る場合に

おいて、かつ、構成国の関連国内指紋データベース内において同時に検索が実施されることを条件として、捜査中の重大犯罪またはテロリスト行為の現場において発見された完全なセットまたは不完全なセットの指紋または掌紋を使用して第 26 条、第 32 条、第 36 条及び第 40 条に従って入れられた警報との関係において SIS の中にある指紋検証法データも検索され得る。

4. それが技術的に可能となったときは、直ちに、かつ、高いレベルの識別の信頼性を確保しつつ、写真及び顔画像は、通常の国境入国地点の過程において、個人を識別するために使用され得る。

その機能が SIS の中に実装される前に、欧州委員会は、要求される技術の可用性、成熟性及び信頼性に関する報告書を提出する。欧州議会は、その報告書に関して協議を受ける。

通常の国境入国地点においてその機能の利用が開始された後、欧州委員会は、写真及び顔画像が個人を識別するために使用され得る別の状況を決定することに関してこの規則を補完するため、第 61 条により委任される行為を採択する権限を与えられる。

第 XIII 章 アクセスの権利並びに警報の見直し

第 44 条 SIS 内のデータへのアクセスの権利をもつ職務権限を有する国内機関

1. 職務権限を有する国内機関は、以下の目的のために、SIS の中に入れられたデータへのアクセスをもち、そのようなデータを直接に、または、SIS データベースの複製物の中で検索する権利をもつ:

(a) 規則(EU) 2016/399 に従い、国境管理;

(b) 関係する構成国内において実施される警察及び税関の検問、並びに、指定された機関によるそのような検問の調整;

(c) 指令(EU) 2016/680 が適用されることを条件として、関係する構成国内におけるテロリスト行為もしくはそれ以外の重大犯罪行為の防止、検知、捜査もしくは訴追、または、刑罰の執行;

(d) 居住許可証及び長期滞在査証を含め、構成国の領土上への第三国国民の入国及び滞在と関連する条件、第三国国民の帰国と関連する条件を審査すること、及び、それらと関連する決定を行うこと、並びに、構成国の領土上に不法入国または不法滞在する第三国国民の検査を実施すること;

(e) その検問を遂行する当局が、欧州議会及び理事会の指令 2013/32/ EU[1]の第 2 条(f)に定義する「決定機関」ではなく、かつ、それが関連するときは、理事会規則(EC) No 377/2004[2]に従って助言を提供する範囲内で、国際的な保護を求める申請をする第三国国民に対する保安検査。

2. SIS 内のデータへのアクセスの権利、及び、そのようなデータを直接に検索する権利は、帰化申請の審査の目的のために、国内法に定める帰化について職責を負う職務権限を有する国内機

[1] 国際的な保護の付与及び取消しの共通手続に関する欧州議会及び理事会の 2013 年 6 月 26 日の指令 2013/32/EU（OJ L 180, 29.6.2013, p.60）

[2] 移民連絡官ネットワークの創設に関する 2004 年 2 月 19 日の理事会規則(EC) No 377/2004（OJ L 64, 2.3.2004, p.1）

関によって行使され得る。

3. SIS 内のデータへのアクセスの権利、及び、そのようなデータを直接に検索する権利は、刑事手続において公訴を提起することについて、及び、個人を起訴する前に刑事法務上の調査をすることについて職責を負う法務当局を含め、国内法に定めるそれらの当局の職務を遂行する際、国内法務当局によって、並びに、それらの当局を統括する当局によっても行使され得る。

4. 本条に示す職務権限を有する機関は、第 56 条第 7 項に示すリストの中に含められる。

第 45 条 自動車登録機関

1. 理事会指令 1999/37/EC[1]に示す自動車の登録証明書の発行について職責を負う構成国内の機関は、自動車及び付帯する自動車登録証及びその登録のためにそれらの機関に対して提示されるナンバープレートが盗まれ、不正流用され、紛失したものであるか否か、そのような文書であると主張されているが偽造であるか否か、または、刑事手続において証拠として求められているものであるか否かを確認する目的のために限り、この規則の第 38 条第 2 項の(a)、(b)、(c)、(m)及び(p)に従って SIS の中に入れられたデータへのアクセスをもつ。

   第 1 副項に示す機関によるデータへのアクセスは、国内法によって規律され、かつ、関係する機関の特定の職務権限内に限定される。

2. 第 1 項に示す機関であって、政府機関である機関は、SIS 内のデータへ直接にアクセスする権利をもつ。

3. 本条第 1 項に示す機関であって、政府機関ではない機関は、第 44 条に示す国内機関の中間媒介を介してのみ、SIS 内のデータへのアクセスをもつ。その国内機関は、データへの直接のアクセスをもち、関係する機関に対し、そのデータを渡す。関係する構成国は、当の機関及びその従業者が、その当局からその機関に対して搬送されたデータの許容され得る利用に関する制限の尊重を要求されることを確保する。

4. 第 39 条は、本条によって得られた SIS へのアクセスに適用してはならない。本条第 1 項に示す機関から警察または法務当局に対する SIS へのアクセスを介して得られた情報の送付は、国内法によって規律される。

第 46 条 船舶及び航空機の登録機関

1. 船舶のエンジンを含め、船舶の登録証明書を発行することまたは船舶の運航管理を確保すること、または、航空機のエンジンを含め、航空機の登録証明書を発行することまたは航空機の運航管理を確保することについて職責を負う構成国内の機関は、登録のためにそれらの機関に提示され、または、その運行管理に服する船舶のエンジンを含め船舶または航空機のエンジンを含め航空機が、盗まれ、不正流用され、紛失したものであるか否か、または、刑事手続において証拠として求められているものであるか否かを確認する目的のために限り、第 38 条第 2 項により SIS の中に入れられた以下のデータへのアクセスをもつ：

   (a) 船舶に関するデータ；

[1] 自動車登録文書に関する 1999 年 4 月 29 日の理事会指令 1999/37/EC（OJ L 138, 1.6.1999, p.57）

(b) 船舶のエンジンに関するデータ;
(c) 航空機に関するデータ;
(d) 航空機のエンジンに関するデータ。

第 1 副項に示す機関によるデータへのアクセスは、国内法によって規律され、かつ、関係する機関の特定の職務権限内に限定される。

2. 第 1 項に示す機関であって、政府機関である機関は、SIS 内のデータへ直接にアクセスする権利をもつ。

3. 本条第 1 項に示す機関であって、政府機関ではない機関は、第 44 条に示す国内機関の中間媒介を介してのみ、SIS 内のデータへのアクセスをもつ。その国内機関は、データへの直接のアクセスをもち、関係する機関に対し、そのデータを渡す。関係する構成国は、当の機関及びその従業者が、その当局からその機関に対して搬送されたデータの許容され得る利用に関する制限の尊重を要求されることを確保する。

4. 第 39 条は、本条によって得られた SIS へのアクセスに適用してはならない。本条第 1 項に示す機関から警察または法務当局に対する SIS へのアクセスを介して得られた情報の送付は、国内法によって規律される。

第 47 条 武器の登録機関

1. 武器の登録証明書の発行について職責を負う構成国内の機関は、第 26 条及び第 36 条に従って SIS の中に入れられた個人に関するデータ及び第 38 条第 2 項に従って SIS の中に入れられた武器に関するデータへのアクセスをもつ。そのアクセスは、その登録を求める者が身柄引渡しもしくは引渡しの目的のための逮捕、または、慎重な検問、質問による検問もしくは個別の検問のために手配されている者であるか否か、または、登録のために提示された武器が刑事手続における差押えまたは証拠としての使用のために求められているものであるか否かを検査する者的のために執行される。

2. 第 1 項に示す機関によるデータへのアクセスは、国内法によって規律され、かつ、関係する機関の特定の職務権限内に限定される。

3. 第1項に示す機関であって、政府機関である機関は、SIS 内のデータへ直接にアクセスする権利をもつ。

4. 本条第 1 項に示す機関であって、政府機関ではない機関は、第 44 条に示す国内機関の中間媒介を介してのみ、SIS 内のデータへのアクセスをもつ。その国内機関は、データへの直接のアクセスをもち、関係する機関に対し、その武器が登録され得る場合に通知する。関係する構成国は、当の機関及びその従業者が、その中間媒介する機関からその機関に対して搬送されたデータの許容され得る利用に関する制限の尊重を要求されることを確保する。

5. 第 39 条は、本条によって得られた SIS へのアクセスに適用してはならない。本条第 1 項に示す機関から警察または法務当局に対する SIS へのアクセスを介して得られた情報の送付は、国内法によって規律される。

第 48 条 Europol による SIS 内のデータへのアクセス

1. 規則(EU) 2016/794 によって設置された欧州連合法執行協力局（Europol）は、その任務を果たすために必要があるときは、SIS の中にあるデータにアクセスし、そのデータを検索する権利をもつ。Europol は、SIRENE マニュアルの条項に従い、補足情報を交換し、かつ、更に要求することもできる。
2. Europol の検索によって、SIS の中に警報が存在することが明らかとなった場合、Europol は、発行構成国に対し、通信インフラにより、かつ、SIRENE マニュアルに定める条項に従い、補足情報の交換を介して、通知する。補足情報の交換のために予定されている機能を Europol が利用可能となるまでの間、Europol は、規則(EU) 2016/794 に定める経路を介して、発行構成国に通知する。
3. Europol は、規則(EU) 2016/794 の第 18 条第 2 項の(a)、(b)及び(c)に示す関係性またはそれ以外の関連性の識別を狙いとし、並びに、戦略分析、主題分析または業務分析のための、補足情報と Europol データベースとの照合及び業務分析プロジェクトの目的のために、構成国から Europol に対して提供された補足情報を処理できる。本条の目的のための補足情報の Europol による処理は、同規則に従って実施される。
4. SIS 内の検索から得られた情報または補足情報の処理から得られた情報の Europol による利用は、発行構成国の同意に服する。その構成国がそのような情報の利用を許容する場合、その情報の Europol による取扱いは、規則(EU) 2016/794 によって規律される。Europol は、発行構成国の同意があり、かつ、データ保護に関する欧州連合法を全面的に遵守する場合に限り、第三国及び第三者に対し、そのような情報を送付する。
5. Europol は:
   (a) 第 4 項及び第 6 項を妨げることなく、SIS のいかなる部分とも接続してはならず、Europol がアクセスをもつ SIS の中に収録されたデータを、Europol によって、または、Europol において運営されるデータの収集及び処理のためのシステムに対して送信してはならず、SIS のいかなる部分についてもダウンロードまたはそれ以外の複製をしてはならない;
   (b) 規則(EU) 2016/794 の第 31 条第 1 項に拘らず、関連する警報が削除された後、遅くとも 1 年以内に、個人データを含む補足情報を削除する。特例により、Europol がそのデータベース内または業務分析プロジェクト内に、その補足情報と関係する案件に関する情報をもつ場合、Europol がその職務を遂行するため、Europol は、例外として、それが必要なときは、その補足情報を記録保存し続けることができる。Europol は、発行構成国及び執行構成国に対し、そのような補足情報の記録保存を継続することを通知し、かつ、その正当化事由を示す;
   (c) 補足情報を含め、SIS の中にあるデータへのアクセスを、彼らの職務の遂行のためにそのようなデータへのアクセスを必要とし、個別の承認を受けた Europol 職員に限定する;
   (d) 第 10 条、第 11 条及び第 13 条に従い、セキュリティ、機密性及び自己監視を確保するための措置を採択及び適用する;
   (e) SIS データを処理することの承認を受けた Europol の職員が、第 14 条第 1 項に従い、適切な訓練及び情報提供を受けることを確保する;並びに、
   (f) 規則(EU) 2016/794 を妨げることなく、SIS の中にあるデータへのアクセス及びそのデータを

検索するための Europol の権利の行使における Europol の活動、並びに、補足情報の交換及び処理における Europol の活動を、欧州データ保護監督官が監視し、見直しできるようにする。

6. Europol は、適正な承認を受けた Europol 職員が直接の検索を実施するため、そのような複製行為が必要な場合において、技術的な目的のためにのみ、SIS からのデータを複製する。この規則は、そのような複製物に適用される。技術上の複製物は、それらのデータが検索中において SIS データを記録保存する目的のためにのみ使用される。データが検索された後、それらの複製物は、削除される。そのような利用は、SIS データの違法なダウンロード行為または複製行為であると判断されてはならない。Europol は、構成国から発された警報データもしくは追加データ、または、CS-SIS からの警報データもしくは追加データを Europol の他のシステム内に複製してはならない。

7. データ処理、自己監視の適法性を確認する目的のために、並びに、データの適正な安全性及び完全性を確保する目的のために、Europol は、第 12 条の条項に従い、SIS への全てのアクセス及び SIS 内の全ての検索の履歴（ログ）を保存する。そのような履歴（ログ）及び文書は、SIS の一部の違法なダウンロード行為または複製行為であると判断されてはならない。

8. 構成国は、Europol に対し、補足情報の交換を介して、テロリスト行為と関連する警報の該当ありを通知する。そのようにすることが、現在進行中の捜査、個人の安全を危険に晒すおそれがあるとき、または、発行構成国の安全上の重要な利益に反するときは、構成国は、例外として、Europol に対して通知しないことが可能である。

9. 第 8 項は、Europol が第 1 項に従って補足情報を取得できる日から適用される。

第 49 条 Eurojust による SIS 内のデータへのアクセス

1. その任務を果たすために必要があるときは、Eurojust の国内構成員及びその補佐官のみが、第 26 条、第 32 条、第 34 条、第 38 条及び第 40 条に従い、SIS の中にあるデータにアクセスし、そのデータを検索する権利をもつ。

2. Eurojust の検索によって、SIS の中に警報が存在することが明らかとなった場合、Eurojust は、発行構成国に対し、通知する。Eurojust は、発行構成国の同意があり、かつ、データ保護に関する欧州連合法を全面的に遵守する場合に限り、第三国及び第三者に対し、そのような検索により入手した情報を送付する。

3. 本条は、データ保護、並びに、Eurojust の国内構成員またはその補佐官によるそのようなデータの無権限の処理または不正確な処理による法的責任に関する欧州議会及び理事会の規則(EU) 2018/1727[1]及び規則(EU) 2018/1725 の条項を妨げず、また、それらの規則による欧州データ保護監督官の権限を妨げない。

4. データ処理の適法性、自己監視を確認する目的のために、並びに、データの適正な安全性及び完全性を確保する目的のために、Eurojust は、第 12 条の条項に従い、SIS への全てのアクセス及び SIS 内の全ての検索の履歴（ログ）を保存する。

[1] 刑事法務上の協力のための欧州連合局（Eurojust）に関する、及び、理事会決定 2002/187/JHA を廃止する欧州議会及び理事会の 2018 年 11 月 14 日の規則(EU) 2018/1727（OJ L 295, 21.11.2018, p.138）

5. Eurojust によって、または、Eurojust において運営されるデータの収集及び処理のためのシステムを SIS のいかなる部分とも接続してはならず、かつ、国内構成員または補佐官がアクセスをもつ SIS の中に収録されたデータを、そのようなシステムに対して送信してはならない。SIS のいかなる部分についてもダウンロードまたは複製してはならない。アクセス及び検索の履歴（ログ）を記録することは、SIS データの違法なダウンロード行為または複製行為であると判断されてはならない。
6. Eurojust は、第 10 条、第 11 条及び第 13 条に従い、セキュリティ、機密性及び自己監視を確保するための措置を採択し、適用する。

第 50 条 欧州国境沿岸警備局、帰国関連の職務に関与する職員のチーム及び移民管理支援チームの構成員による SIS 内のデータへのアクセス

1. 規則(EU) 2016/1624 の第 40 条第 8 項に従い、同規則第 2 項の(8)及び(9)に示すチームの構成員は、彼らの任務の範囲内において、かつ、この規則の第 44 条第 1 項による検問を実施することを彼らが承認されていること、及び、この規則の第 14 条第 1 項に従って必要な訓令を受けたことを条件として、彼らの職務の遂行のために必要な限り、かつ、個別の業務遂行のための業務遂行計画によって要求されるように、SIS の中にあるデータにアクセスし、そのデータを検索する権利をもつ。SIS の中にあるデータへのアクセスは、チームの他の構成員に対して拡大してはならない。
2. 第 1 項に示すチームの構成員は、技術インタフェイスを介して、第 1 項による SIS の中にあるデータにアクセスし、そのデータを検索する権利を行使する。技術インタフェイスは、欧州国境沿岸警備局によって設置及び維持管理され、かつ、中央 SIS への直接のアクセスを許容する。
3. 本条第 1 項に示すチームの構成員の検索によって、SIS の中に警報が存在することが明らかとなった場合、発行構成国は、そのことの通知を受ける。規則(EU) 2016/1624 の第 40 条に従い、そのチームの構成員は、その職務が遂行されているホスト構成国の帰国関連職務に関与する国境警備隊員または職員の指示の下においてのみ、かつ、原則として、その立会の下においてのみ、SIS の中の警報に対応して行動する。そのホスト構成国は、そのチームの構成員に対し、そのホスト構成国の代わりに行動することを承認できる。
4. データ処理の適法性、自己監視を確認する目的のために、並びに、データの適正な安全性及び完全性を確保する目的のために、欧州国境沿岸警備局は、第 12 条の条項に従い、SIS への全てのアクセス及び SIS 内の全ての検索の履歴（ログ）を保存する。
5. 欧州国境沿岸警備局は、第 10 条、第 11 条及び第 13 条に従い、セキュリティ、機密性及び自己監視を確保するための措置を採択し、適用し、かつ、本条第 1 項に示すチームがそれらの措置を適用することを確保する。
6. 本条のいかなる条項も、データ保護、または、欧州国境沿岸警備局によるデータの無権限の処理または不正確な処理による欧州国境沿岸警備局の法的責任に関する規則(EU) 2016/1624 の条項に影響を与えるものとして解釈してはならない。
7. 第 2 項を妨げることなく、第 1 項に示すチームによって、または、欧州国境沿岸警備局によって運営されるデータの収集及び処理のためのシステムを SIS のいかなる部分とも接続してはならず、かつ、それらのチームがアクセスをもつ SIS の中に収録されたデータを、そのようなシステム

に対して送信してはならない。SIS のいかなる部分についてもダウンロードまたは複製してはならない。アクセス及び検索の履歴（ログ）を記録することは、SIS データの違法なダウンロード行為または複製行為であると判断されてはならない。

8. 欧州国境沿岸警備局は、SIS の中にあるデータへのアクセス及びそのデータを検索するための彼らの権利の行使における本条に示すチームの活動を、欧州データ保護監督官が監視し、見直しできるようにする。このことは、規則(EU) 2016/794 の他の情報を妨げてはならない。

第 51 条 Europol、Eurojust 及び欧州国境沿岸警備局による SIS の利用の評価

1. 欧州委員会は、少なくとも 5 年毎に、Europol、Eurojust の国内構成員及びその補佐官並びに第 50 条第 1 項に示すチームによる業務遂行及び SIS の利用の評価を実施する。
2. Europol、Eurojust 及び欧州国境沿岸警備局は、その評価から得られる判断及び勧告の十分なフォローアップを確保する。
3. 評価結果及びそのフォローアップに関する報告書は、欧州議会及び理事会に対して送付される。

第 52 条 アクセスの適用範囲

Europol、Eurojust の国内構成員及びその補佐官、並びに、規則(EU) 2016/1624 の第 2 条の(8)及び(9)に示すチームの構成員を含め、エンドユーザは、彼らの職務を遂行するために彼らが必要とするデータに限り、アクセスする。

第 53 条 個人に関する警報の見直し期間

1. 個人に関する警報は、その警報が入れられた目的を達成するために必要な期間内に限り、保存される。
2. 構成国は、第 26 条並びに第 32 条第 1 項の(a)及び(b)の目的のために、5 年の期間で、個人に関する警報を入れることができる。その発行構成国は、5 年以内に、その警報を保持すべき必要性を見直す。
3. 構成国は、第 34 条並びに第 40 条の目的のために、3 年の期間で、個人に関する警報を入れることができる。その発行構成国は、3 年以内に、その警報を保持すべき必要性を見直す。
4. 構成国は、第 32 条第 1 項の(c)、(d)及び(e)並びに第 36 条の目的のために、1 年の期間で、個人に関する警報を入れることができる。その発行構成国は、1 年以内に、その警報を保持すべき必要性を見直す。
5. 各構成国は、それが適切なときは、その国内法に従い、より短い見直し期間を定める。
6. 第 2 項、第 3 項及び第 4 項に示す見直し期間中、発行構成国は、記録される包括的な個別評価により、その警報が入れられた目的のために必要かつ比例的であることが明らかな場合、その見直し期間よりも長くその個人に関する警報を保持することを決定できる。そのような場合、その延長に第 2 項、第 3 項または第 4 項が適用される。そのような延長は、CS-SIS に対して通知される。

7. 発行構成国が CS-SIS に対して第 6 項による延長を通知した場合を除き、第 2 項、第 3 項及び第 4 項に示す見直し期間の経過後、個人に関する警報は、自動的に削除される。CS-SIS は、発行構成国に対し、自動的に、その 4 か月前に、データ削除の予定を通知する。
8. 構成国は、本条の第 6 項に従って保持期間が延長された個人に関する警報の数の統計を保存し、かつ、要請に応じて、第 69 条に示す監督機関に対し、その統計を送付する。
9. 個人に関する警報がその目的を達成しており、それゆえ、削除されるべきであることが SIRENE 事務局に明らかになったときは、その SIRENE 事務局は、直ちに、その警報を作成した機関に対して通知する。その機関は、その警報が削除されたこと、もしくは、その警報が削除されることを、または、その警報の保持の理由を示す回答をするために、その通知を受領した時から 15 暦日をもつ。その 15 日の期間の最終日までに何らの回答もない場合、その SIRENE 事務局は、その警報が削除されたことを確認する。国内法に基づいて許容される場合、その警報は、SIRENE 事務局によって削除される。SIRENE 事務局は、その SIRENE 事務局の監督機関に対し、その SIRENE 事務局が本項に基づいて行動する際に直面した問題の再発を報告する。

第 54 条 対象物に関する警報の見直し期間

1. 対象物に関する警報は、その警報が入れられた目的を達成するために必要な期間内に限り、保存される。
2. 構成国は、第 36 条並びに第 38 条の目的のために、10 年の期間で、対象物に関する警報を入れることができる。その発行構成国は、10 年以内に、その警報を保持すべき必要性を見直す。
3. それらの対象物に関する警報が個人に関する警報とリンクされている場合、第 26 条、第 32 条、第 34 条及び第 36 条に従って入れられた対象物に関する警報は、第 53 条により見直される。そのような警報は、個人に関する警報が保存されている間に限り、保存される。
4. 第 2 項及び第 3 項に示す見直し期間中、発行構成国は、その警報が入れられた目的のために必要かつ比例的であることが明らかな場合、その見直し期間よりも長くその対象物に関する警報を保持することを決定できる。そのような場合、第 2 項または第 3 項がしかるべく適用される。
5. 欧州委員会は、一定の類型の対象物に関する警報のより短い見直し期間を定めるための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。
6. 構成国は、本条の第 4 項に従って保持期間が延長された対象物に関する警報の数の統計を保存する。

第 XIV 章 警報の削除

第 55 条 警報の削除

1. 第 26 条による身柄引渡しまたは引渡しの目的のための逮捕に関する警報は、その者がその発行構成国の職務権限を有する機関に対して身柄引渡しまたは引渡しされたときは、削除される。それらの警報は、その警報が基礎とした法務上の決定が、国内法に従い、職務権限を有する法務当局によって破棄されたときにおいても、削除される。それらの警報は、第 53 条に従い、その警報が期間満了となった場合においても、削除される。

2. 失踪者に関する警報または第 32 条により旅行が阻止される必要性のある脆弱性のある者に関する警報は、以下の規定に従い、削除される：
   (a) 失踪児童及び連れ去りのリスクに直面している児童に関し、警報は、以下の場合に削除される：
      (i) その児童が発見された場合もしくは送還された場合、または、執行構成国の職務権限を有する機関がその児童の案件に関する決定を行った場合のような、その案件の解決；
      (ii) 第 53 条によるその警報の期間満了；または、
      (iii) 発行構成国の職務権限を有する機関による決定；
   (b) 成人の失踪者に関し、何らの保護措置も要しない場合、警報は、以下の場合に削除される：
      (i) 執行構成国によりそれらの者の所在が確認された場合、執られるべき行動の執行；
      (ii) 第 53 条によるその警報の期間満了；または、
      (iii) 発行構成国の職務権限を有する機関による決定；
   (c) 成人の失踪者に関し、保護措置を要する場合、警報は、以下の場合に削除される：
      (i) その者が保護の下に置かれている場合、執られるべき行動の執行；
      (ii) 第 53 条によるその警報の期間満了；または、
      (iii) 発行構成国の職務権限を有する機関による決定；
   (d) 彼ら自身の保護のために旅行が阻止される必要性のある脆弱性のある者及び旅行が阻止される必要性のある児童に関し、警報は、以下の場合に削除される：
      (i) その者が保護の下に置かれている場合、執られるべき行動の執行；
      (ii) 第 53 条によるその警報の期間満了；または、
      (iii) 発行構成国の職務権限を有する機関による決定。

   国内法を妨げることなく、職務権限を有する機関による決定に従い、その者が施設収容された場合、当該の者が送還されるまでの間、警報が保持され得る。
3. 第 34 条により刑事手続を求められている者に関する警報は、以下の場合に削除される：
   (a) 発行構成国の職務権限を有する機関に対するその者の所在の連絡；
   (b) 第 53 条によるその警報の期間満了；または、
   (c) 発行構成国の職務権限を有する機関による決定。

   (a)に示す連絡中の情報に基づいて行動できない場合、発行構成国の SIRENE 事務局は、問題を解決するため、執行構成国の SIRENE 事務局に対して通知する。

   発行構成国に対して住所の該当ありが通知された場合において、その後に、同じ執行構成国内の該当ありによって同じ住所が明らかにされた場合、その該当ありは、執行構成国内において記録されるが、その住所及び補足情報は、いずれも、発行構成国に対して送付されない。そのような場合、執行構成国は、発行構成国に対し、再度の該当ありを通知し、かつ、発行構成国は、その警報を保持する必要性の包括的な個別評価を実施する。
4. 第 36 条による慎重な検問、質問による検問及び個別の検問に関する警報は、以下の場合に削除される：
   (a) 第 53 条によるその警報の期間満了；または、
   (b) 発行構成国の職務権限を有する機関によるその警報を削除する決定。
5. 第 38 条による刑事手続における差押えまたは証拠としての使用のための対象物に関する警

報は、以下の場合に削除される：

(a) 関係する SIRENE 事務局間において必要な補足情報のフォローアップ交換が行われた後のその対象物の差押えもしくはそれと均等な措置の実施、または、その対象物が別の法務上の手続もしくは行政上の手続の対象となること；

(b) 第 53 条によるその警報の期間満了；または、

(c) 発行構成国の職務権限を有する機関による決定。

6. 第 40 条による未認知手配者に関する警報は、以下の場合に削除される：

(a) その個人の識別；

(b) 第 53 条によるその警報の期間満了；または、

(c) 発行構成国の職務権限を有する機関による決定。

7. その警報が個人に関する警報とリンクされている場合、第 26 条、第 32 条、第 34 条及び第 36 条に従って入れられた対象物に関する警報は、本条に従ってその個人に関する警報が削除されるときは、削除される。

第 XV 章 一般的なデータ保護原則

第 56 条 SIS データの処理

1. 構成国は、第 26 条、第 32 条、第 34 条、第 36 条、第 38 条及び第 40 条に示す各類型の警報に定める目的のために限り、第 20 条に示すデータを処理する。

2. 第 44 条に示す職務権限を有する機関が直接の検索を実施するため、そのような複製が必要となる場合において、技術的な目的のために限り、データが複製される。この規則は、それらの複製物に適用される。構成国は、別の構成国によって入れられた警報データまたは追加データを、その構成国の N.SIS または CS-SIS から、別の国内データファイルの中に複製してはならない。

3. オフラインのデータベースの中で生成される第 2 項に示す技術複製物は、48 時間を超えて保持されてはならない。

構成国は、それらの複製物の最新の登録簿を維持し、その登録簿をその構成国の監督機関が利用できるようにし、かつ、それらの複製物に関し、この規則、とりわけ、第 10 条が適用されることを確保する。

4. 第 44 条に示す職務権限を有する国内機関による SIS 内のデータへのアクセスは、その機関の職務権限の制限内に限り、かつ、適正に承認を受けた職員に対してのみ、承認される。

5. この規則の第 26 条、第 32 条、第 34 条、第 36 条、第 38 条及び第 40 条に定める警報に関し、そのデータが SIS の中に入れられた目的以外の目的のための構成国による SIS データの処理は、個別の案件と関連性のあるものでなければならず、かつ、国家安全保障上の重大な根拠に基づき、または、重大犯罪を防止する目的のため、公共政策及び公共の安全に対する差し迫った重大な脅威を防止するための必要性によって正当化されなければならない。その目的のために、発行構成国から事前の承認を得なければならない。

6. 本条の第 1 項ないし第 5 項を遵守しない SIS データの利用は、各構成国の国内法に基づき、濫用と判断され、かつ、第 73 条に従い、制裁に服する。

7. 各構成国は、eu-LISA に対し、この規則によって SIS 内のデータの直接の検索の承認を受け

ているその構成国の職務権限を有する機関のリスト、並びに、そのリストの変更を送付する。そのリストは、個々の機関について、どのデータが検索され得るのか、及び、どの目的のために検索され得るのかを示す。eu-LISA は、そのリストが、年次で、EU 官報上で公示されることを確保する。eu-LISA は、年次の公示の間に構成国から送付された変更を含む継続的にアップデートされるリストを、その Web サイト上において維持する。

8. 欧州連合法が特別の条項を定めていない範囲内において、各構成国の法律は、その構成国の N.SIS の中にあるデータに適用される。

第 57 条 SIS データ及び国内ファイル

1. 第 56 条第 2 項は、その構成国の領土上において執られる行動との関係において、その構成国の国内ファイルの中に SIS データを保存するための構成国の権利を妨げてはならない。国内法の特別の条項がより長期の保持期間を定めている場合を除き、そのようなデータは、最長で 3 年間、国内ファイルの中で保存される。
2. 第 56 条第 2 項は、当該構成国によって SIS の中に入れられた特定の警報に含まれているデータを、その構成国の国内ファイルの中で保存するための構成国の権利を妨げてはならない。

第 58 条 警報の不執行の場合の情報

要求される行動を遂行できない場合、その行動を要求された構成国は、発行構成国に対し、補足情報の交換を介して、直ちに、通知する。

第 59 条 SIS 内のデータの品質

1. 発行構成国は、データが、正確であり、最新のものであり、かつ、SIS の中に適法に入れられ、記録保存されることを確保することについて職責を負う。
2. 発行構成国が、第 20 条第 3 項に列挙する関連追加データまたは関連修正データを取得したときは、その発行構成国は、遅滞なく、その警報を完全なものとし、または、修正する。
3. 発行構成国が SIS の中に入れたデータを修正し、追加し、訂正し、アップデートし、または、削除することが認められるのは、その発行構成国だけである。
4. 発行構成国以外の構成国が、第 20 条第 3 項に列挙する関連追加データまたは関連修正データをもつ場合、その構成国は、発行構成国に対し、その発行構成国がその警報を完全なものとし、または、修正できるようにするため、補足情報の交換を介して、遅滞なく、そのデータを送付する。追加または修正が行われる場合、その個人に関するデータは、その個人の同一性が確認される場合に限り、送付される。
5. 発行構成国以外の構成国が、あるデータ項目が事実として不正確であること、または、違法に記録保存されたことを示す証拠をもつ場合、その構成国は、発行構成国に対し、可能な限り速やかに、かつ、その証拠に気づいたときから 2 業務日以内に、補足情報の交換を介して、そのことの情報を提供する。その発行構成国は、その情報を確認し、かつ、それが必要なときは、遅滞なく、当の項目を訂正または削除する。

6. 本条第 5 項に示す証拠が最初に明らかにされた時から 2 か月以内に構成国間で合意に達することができない場合、その警報を入れたのではない構成国は、判断を得るため、関係する監督機関及び欧州データ保護監督官に対し、第 71 条に従った協力の措置により、その案件を付託する。
7. 構成国は、ある者が、彼または彼女が警報の想定する対象者ではない旨の不服を申立てた場合において、補足情報を交換する。確認の結果により、警報の想定する対象者がその不服申立人ではないことが明らかとなった場合、その不服申立人は、第 62 条に定める措置、及び、第 68 条第 1 項に基づく救済の権利の通知を受ける。

第 60 条 セキュリティインシデント

1. SIS の安全性を損なう影響をもつ出来事、もしくは、もち得る出来事、または、SIS データもしくは補足情報に対して毀損または喪失を発生させ得る出来事は、特に、データへの違法なアクセスが発生した可能性がある場合、または、データの可用性、完全性及び機密性が危殆に瀕した場合、もしくは、危殆に瀕した可能性のある場合においては、セキュリティインシデントであると判断される。
2. セキュリティインシデントは、迅速であり、効果的であり、かつ、適正な対応を確保する態様によって管理される。
3. 規則(EU) 2016/679 の第 33 条または指令(EU) 2016/680 の第 30 条による個人データの侵害の通知及び連絡を妨げることなく、構成国、Europol、Eurojust 及び欧州国境沿岸警備局は、欧州委員会、eu-LISA、職務権限を有する監督機関及び欧州データ保護監督官に対し、遅滞なく、セキュリティインシデントを通知する。eu-LISA は、欧州委員会及び欧州データ保護監督官に対し、遅滞なく、中央 SIS と関連する全てのセキュリティインシデントを通知する。
4. 構成国内もしくは eu-LISA 内の SIS の運営、入れられたデータもしくは他の構成国から送付されたデータの可用性、完全性及び機密性、または、交換された補足情報に対して影響をもつセキュリティインシデントまたは影響をもつ可能性のあるセキュリティインシデントに関する情報は、遅滞なく、全ての構成国に対して提供され、かつ、eu-LISA から提供されるインシデント管理計画を遵守して報告される。
5. 構成国及び eu-LISA は、セキュリティインシデントが発生した場合、共働する。
6. 欧州委員会は、欧州議会及び理事会に対し、直ちに、重大なインシデントを報告する。それらの報告は、適用される安全規則に従い、EU 取扱注意（EU RESTRICTED/RESTREINT UE）として区分される。
7. セキュリティインシデントがデータの濫用によるものである場合、構成国、Europol、Eurojust 及び欧州国境沿岸警備局は、第 73 条に従い、制裁が加えられることを確保する。

第 61 条 類似する特徴をもつ個人間の区別

1. 新たな警報が入れられた後、同じ識別子の記述をもつ者に関して SIS の中に既に警報が存在することが明らかとなった場合、SIRENE 事務局は、その 2 つの警報の対象者が同一の者であるか否かを照合するため、12 時間以内に、補足情報の交換を介して、発行構成国と連絡をとる。

2. その照合により、新たな警報の対象者と既に SIS の中に入れられている警報の対象者とが確実に同一の者であることが明らかとなった場合、その SIRENE 事務局は、第 23 条に示す複数の警報の入力に関する手続を適用する。
3. その照合の結果が、事実として 2 人の異なる者が存在するというものである場合、その SIRENE 事務局は、誤認を避けるために必要となるデータを追加することにより、第 2 の警報を入れることを求める要請を承認する。

第 62 条 濫用された識別子を取り扱う目的のための追加データ

1. 警報の対象者として想定されている者と識別子が濫用された者との間に混同が生じている可能性がある場合、発行構成国は、その識別子が濫用された者の明示の同意に従い、誤認による負の結果を避けるため、後者の者に関するデータをその警報に追加する。その識別子が濫用された者は、追加される個人データの処理と関連する彼または彼女の同意を撤回する権利をもつ。
2. その識別子が濫用された者と関連するデータは、以下の目的のためにのみ、使用される：
   (a) その識別子が濫用された者と警報の対象者として想定されている者とを職務権限を有する機関が区別できるようにするため；並びに、
   (b) その識別子が濫用された者が彼または彼女の同一性を証明できるようにするため、及び、彼または彼女の識別子が濫用されたことを立証できるようにするため。
3. 本条の目的のために、かつ、個々のデータの類型について、その識別子が濫用された者の明示の同意に従い、その識別子が濫用された者の以下の個人データに限り、SIS の中に入れられ、かつ、別の目的のために処理され得る：
   (a) 姓；
   (b) 名；
   (c) 出生時の名；
   (d) 別に入れられた可能性のある過去に使用していた名及び別名；
   (e) 変更されない、特定の、客観的で物理的な特徴；
   (f) 出生の場所；
   (g) 出生の日；
   (h) 性；
   (i) 写真及び顔画像；
   (j) 指紋、掌紋またはその両方；
   (k) 保有している国籍；
   (l) その者の身分証明書の類型；
   (m) その者の身分証明書の発行国；
   (n) その者の身分証明書の番号；
   (o) その者の身分証明書の発行日；
   (p) その者の住所；
   (q) その者の父の名；
   (r) その者の母の名。
4. 欧州委員会は、本条第 3 項に示すデータの入力及び別の目的のための処理のために必要と

なる技術規則を定め、策定するための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

5. 第 3 項に示すデータは、対応する警報と同時に、または、その者がそのように要求する場合、それよりも早い時点で、削除される。
6. 第 3 項に示すデータにアクセスできるのは、対応する警報へのアクセスの権利をもつ機関のみである。それらの機関は、誤認を避ける目的のために限り、そのようにできる。

第 63 条 複数の警報間のリンク

1. 構成国は、その構成国が SIS の中に入れる複数の警報の間のリンクを作成できる。そのようなリンクの効果は、複数の警報の間の関連性を構築することである。
2. リンクの作成は、リンクされた個々の警報に基づいて執られる個別の行動、または、リンクされた個々の警報の見直し期間を害してはならない。
3. リンクの作成は、この規則に定めるアクセスの権利を害してはならない。一定の類型の警報へのアクセスの権利をもたない機関は、その機関がアクセスをもたない警報へのリンクを見ることが可能であってはならない。
4. 構成国は、運営上の必要性が存在する場合、複数の警報の間のリンクを作成する。
5. ある構成国が、別の構成国による複数の警報の間のリンクの作成がその構成国の国内法またはその構成国の国際的な義務と適合しないと判断する場合、その構成国は、その構成国の領土内から、または、その構成国の領土外に所在するその構成国の機関によって、そのリンクへのアクセスができないことを確保するために必要となる措置を講ずることができる。
6. 欧州委員会は、警報間のリンク設置に関する技術規則を定め、策定するための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 64 条 補足情報の目的及び保持期間

1. 構成国は、補足情報の交換を支援するために、SIRENE 事務局において、警報を発生させた決定の参照を保存する。
2. 補足情報の交換の結果として SIRENE 事務局によってファイルの中に保存される個人データは、その個人データが供給された目的を達成するために必要であるような期間に限り、保存される。それらの個人データは、いかなる場合においても、関連する警報が SIS の中から削除された時から遅くとも 1 年以内に削除される。
3. 第 2 項は、当該構成国が入れた特定の警報と関連するデータ、または、その構成国の領土上において執られた行動と関係する警報と関連するデータを国内ファイルの中で保存するための構成国の権利を妨げてはならない。それらのデータがそれらのファイルの中で保存され得る期間は、国内法によって規律される。

第 65 条 第三国への個人データの移転

SIS の中で処理されるデータ及びこの規則により交換される関連補足情報は、第三国または国

際機関に対して移転してはならず、または、第三国または国際機関が利用できるようにしてはならない。

第 XVI 章　データ保護

第 66 条　適用される立法

1. 規則(EU) 2018/1725 は、この規則に基づく eu-LISA、欧州国境沿岸警備局及び Eurojust による個人データの処理に適用される。規則(EU) 2016/794 は、この規則に基づく Europol による個人データの処理に適用される。
2. 指令(EU) 2016/680 は、公共の安全に対する脅威に対抗する防護及びその脅威の防止を含め、犯罪行為の防止、検知、捜査もしくは訴追または刑罰の執行の目的のために、職務権限を有する機関によるこの規則に基づく個人データの処理に適用される。

第 67 条　アクセス、不正確なデータの訂正及び違法に記録保存されたデータの削除の権利

1. データ主体は、規則(EU) 2016/679 の第 15 条、第 16 条及び第 17 条、並びに、指令(EU) 2016/680 の第 14 条、第 16 条第 1 項及び第 2 項に定める権利を行使できる。
2. 発行構成国以外の構成国は、その構成国が発行構成国に対してその発行構成国の意見を述べる機会を先に与えた場合に限り、データ主体に対し、処理されているいずれかのデータ主体の個人データに関する情報を提供できる。構成国間の連絡は、補足情報の交換を介して行われる。
3. 構成国は、そのような全部または一部の制限が、以下のために、関係するデータ主体の基本的な権利及び正当な利益に適正に配慮し、民主主義社会において必要かつ比例的な措置を構成する範囲内で、かつ、その限りにおいて、国内法に従い、データ主体に対して情報の全部または一部を提供しない決定を行う:
   (a) 公的調査もしくは法律上の調査、捜査または手続の妨げとなることを避けるため;
   (b) 犯罪行為の防止、検知、捜査もしくは訴追または刑罰の執行の阻害を避けるため;
   (c) 公共の安全を防護するため;
   (d) 国家安全保障を防護するため;または、
   (e) 他の者の権利及び自由を保護するため。

   第 1 副項に示す各場合において、構成国は、データ主体に対し、書面により、遅滞なく、アクセスの拒否または制限及びその拒否または制限の理由を通知する。第 1 副項の(a)ないし(e)に定める理由のいずれかをその提供が損ねる場合、そのような情報提供は、省略され得る。構成国は、データ主体に対し、監督機関に異議を申し立てることができること、または、司法救済を求めることができることを通知する。

   構成国は、データ主体に対して情報を提供しない決定が基礎とする事実に関する理由及び法律上の理由を文書化する。その情報は、監督機関に対し、利用できるようにされる。

   そのような場合、データ主体は、職務権限を有する監督機関を介して、彼または彼女の権利を行使できる。

4. アクセス、訂正または削除を求める申請の後、構成国は、データ主体に対し、可能な限り速やかに、かつ、いかなる場合においても、規則(EU) 2016/679 の第 12 条第 3 項に示す期限内に、本条に基づく権利の行使に与えられたフォローアップに関して通知する。

第 68 条 救済

1. 規則(EU) 2016/679 及び指令(EU) 2016/680 の救済に関する条項を妨げることなく、いかなる者も、構成国の法律に基づき、彼または彼女と関連する警報と関係するアクセス、訂正、削除、情報提供の獲得または弁償の獲得のために、裁判所を含め、職務権限を有する機関において訴訟を提起できる。
2. 構成国は、第 72 条を妨げることなく、本条の第 1 項に示す裁判所または機関によって行われた確定的な判断の執行を相互に実施する。
3. 構成国は、欧州データ保護委員会に対し、以下に関し、年次で報告する:
   (a) データ管理者に対して申立てられたアクセス要求の数、及び、データへのアクセスが与えられた案件の数;
   (b) 監督機関に対して申立てられたアクセス要求の数、及び、データへのアクセスが与えられた案件の数;
   (c) データ管理者に対して申立てられた不正確なデータの訂正の要求及び違法に記録保存されたデータの削除の要求の数、及び、データが訂正または削除された案件の数;
   (d) 監督機関に対して申立てられた不正確なデータの訂正の要求及び違法に記録保存されたデータの削除の要求の数;
   (e) 開始された裁判手続の数;
   (f) 裁判所が申立人に有利に判断した事件の数;
   (g) 発行構成国によって入れられた警報に関し、他の構成国の裁判所または機関によって行われた確定的な判断の相互承認案件に関する所見。

   本項に示す報告のための雛形は、欧州委員会によって策定される。
4. 構成国からの報告は、第 71 条第 4 項に示す共同報告書の中に含められる。

第 69 条 N.SIS の監督

1. 構成国は、構成国から指定され、かつ、規則(EU) 2016/679 の第 VI 章または指令(EU) 2016/680 の第 VI 章に示す権限を与えられた独立の監督機関が、その構成国における SIS 内の個人データ処理の適法性、その構成国の領土からの送信、並びに、その構成国の領土における補足情報の交換及び別の目的のための処理を監視することを確保する。
2. その監督機関は、国際的な監査基準に従い、少なくとも 4 年毎に、その構成国の N.SIS におけるデータ処理業務の監査が実施されることを確保する。その監査は、監督機関によって行われ、または、監督機関は、独立のデータ保護監査人に対して監査を命ずる。監督機関は、常時、独立の監査人の監督を維持し、かつ、その監査人について責任を負う。
3. 構成国は、その構成国の監督機関が、この規則に基づきその機関に委託された職務を満たすために十分な資源をもつこと、及び、生体データの十分な知識をもつ者からの助言へのアクセス

をもつことを確保する。

第 70 条 eu-LISA の監督

1. 欧州データ保護監督官は、eu-LISA による個人データの処理の監視について、及び、この規則に従ってそれが実施されることの確保について職責を負う。規則(EU) 2018/1725 の第 57 条及び第 58 条に示す職務及び権限がしかるべく適用される。
2. 欧州データ保護監督官は、国際的な監査基準に従い、少なくとも 4 年毎に、eu-LISA による個人データ処理の監査を実施する。その監査に関する報告書は、欧州議会、理事会、eu-LISA、欧州委員会及び監督機関に対して送付される。eu-LISA は、その報告書が採択される前に、意見を述べる機会を与えられる。

第 71 条 監督機関と欧州データ保護監督官との間の協力

1. 監督機関及び欧州データ保護監督官は、それらそれぞれの職務権限の範囲内において各自行動し、それらの職責の枠組み内において積極的に協力し、かつ、SIS の調整された監督を確保する。
2. 監督機関及び欧州データ保護監督官は、それらそれぞれの職務権限の範囲内において各自行動し、必要に応じて、関連情報を交換し、監査及び調査を実施する際に相互に補助し、この規則及びそれ以外の適用可能な欧州連合の法令の解釈または適用における問題点を検討し、独立の監督の実行を通じて、または、データ主体の権利の行使を通じて明らかにされた問題を調査研究し、問題点を共同して解決するための整合性のある提案を策定し、かつ、データ保護の権利の認識を向上させる。
3. 第 2 項に定める目的のために、監督機関及び欧州データ保護監督官は、欧州データ保護委員会の一部として、少なくとも 1 年に 2 回、会合する。それらの会合の費用及び開催準備は、欧州データ保護委員会の負担とする。最初の会合において、手続規則が採択される。必要に応じ、別の作業手法が策定される。
4. 欧州データ保護委員会から、年次で、欧州議会、理事会及び欧州委員会に対し、調整された監督に関する共同活動報告書が提出される。

第 XVII 章 法的責任及び制裁

第 72 条 法的責任

1. 規則(EU) 2016/679、指令(EU) 2016/680 及び規則(EU) 2018/1725 に基づく損害賠償の権利及び法的責任を妨げることなく:
   (a) 構成国による N.SIS の利用を介する違法な個人データ処理業務の結果として、または、それ以外の構成国によるこの規則と適合しない行為の結果として、物的損害または非物的損害を被った個人または構成国は、当該構成国から損害賠償を受ける権利をもち;かつ、
   (b) eu-LISA によるこの規則と適合しない行為の結果として、物的損害または非物的損害を被っ

た個人または構成国は、eu-LISA から損害賠償を受ける権利をもつ。

構成国または eu-LISA は、その損害を発生させた出来事に関してそれらが責任を負わないことを証明したときは、第 1 副項に基づくそれらの責任の全部または一部を免れる。

2. この規則に基づく構成国の義務の不遵守が SIS に損害を発生させた場合、eu-LISA または SIS に関与する別の構成国が、その損害の発生の防止またはその影響のミニマム化のための合理的な措置を講じなかった場合を除き、かつ、その範囲内において、当該構成国は、そのような損害に関し、法的責任を負う。

3. 構成国を相手方とする第 1 項及び第 2 項に示す損害の賠償を求める請求は、当該構成国の国内法によって規律される。eu-LISA を相手方とする第 1 項及び第 2 項に示す損害の賠償を求める請求は、諸条約に定める条件に服する。

第 73 条 制裁

構成国は、この規則に反する SIS データの濫用またはそのようなデータの処理もしくは補足情報の交換が国内法に従って制裁を受け得ることを確保する。

定められる制裁は、効果的であり、比例的であり、かつ、抑止力のあるものとする。

第 XVIII 章 最終規定

第 74 条 監視及び統計

1. eu-LISA は、出力、費用対効果、セキュリティ及びサービス品質と関連する目的に照らし、SIS の稼働を監視するための手続が設けられることを確保する。

2. 技術上の維持管理、報告、データの品質の報告及び統計の目的のために、eu-LISA は、中央 SIS の中で遂行される処理業務と関連する必要な情報へのアクセスをもつ。

3. eu-LISA は、構成国毎のもの及び集約されたものの両者により、警報の類型毎の記録の数を示す日別、月次及び年次の統計を作成する。eu-LISA は、警報の類型毎の該当ありの数、SIS が何回検索されたか、並びに、警報の入力、アップデートまたは削除の目的のために SIS が何回アクセスされたかに関し、構成国毎のもの及び集約されたものの両者による年次報告書も提供する。その統計は、いかなる個人データも含めてはならない。年次統計報告書は、公表される。

4. 構成国、Europol、Eurojust 及び欧州国境沿岸警備局は、eu-LISA 及び欧州委員会に対し、第 3 項、第 6 項、第 8 項及び第 9 項に示す報告書を作成するために必要な情報を提供する。

5. この情報は、船舶のエンジンを含め、船舶の登録証明書を発行することについて職責を負う構成国内の機関または船舶の運航管理を確保することについて職責を負う構成国内の機関；航空機のエンジンを含め、航空機の登録証明書を発行することまたは航空機の運航管理を確保することについて職責を負う構成国内の機関；並びに、武器の登録証明書を発行することについて職責を負う構成国内の機関によって実施され、または、その代わりに実施された検索の数に関する区分された統計を含める。その統計は、警報の類型毎の該当ありの数も示す。

6. eu-LISA は、欧州議会、理事会、構成国、欧州委員会、Europol、Eurojust、欧州国境沿岸警備局及び欧州データ保護監督官に対し、eu-LISA が作成した統計報告書を提供する。

規則(EU) No 1053/2013 の目的のための場合を含め、欧州連合の法的行為の実装を監視するため、欧州委員会は、eu-LISA が、定期的またはアドホックに、SIS の業務遂行能力、SIS の利用及び補足情報の交換に関する追加的な個別の統計報告書を提供することを要求できる。

欧州国境沿岸警備局は、eu-LISA が、定期的またはアドホックに、規則(EU) 2016/1624 の第 11 条及び第 13 条に示すリスク分析及び脆弱性評価を実施する目的のための追加的な個別の統計報告書を提供することを要求できる。

7. 第 15 条第 4 項並びに本条第 3 項、第 4 項及び第 6 項の目的のために、eu-LISA は、第 15 条第 4 項及び本条第 3 項に示すデータを収録し、個人の識別を許容せず、かつ、欧州委員会及び本条第 6 項に示す部局が特注の報告書及び統計を得ることができるようにする中央リポジトリを、eu-LISA の技術サイト内に構築し、実装し、かつ、ホストする。要請に基づき、eu-LISA は、構成国、欧州委員会、Europol、Eurojust 及び欧州国境沿岸警備局に対し、それらの職務を遂行するために要する範囲内で、通信インフラを介する安全なアクセスにより、その中央リポジトリへのアクセスを与える。eu-LISA は、報告及び統計の目的のために限り、その中央リポジトリがアクセスされることを確保するためのアクセス管理及び個別の利用者プロファイルを実装する。

8. 第 79 条第 5 項第 1 副項によるこの規則の適用の日から 2 年後、及び、その後は 2 年毎に、eu-LISA は、欧州議会及び理事会に対し、そのセキュリティを含め、中央 SIS 及び通信インフラの技術上の稼働、AFIS、構成国間における 2 国間または多国間の補足情報の交換に関する報告書を提出する。その報告書は、その技術が利用可能となった後、個人を識別するための顔画像の使用の評価も含める。

9. 第 79 条第 5 項第 1 副項によるこの規則の適用の日から 2 年後、及び、その後は 4 年毎に、欧州委員会は、中央 SIS 及び構成国間における 2 国間または多国間の補足情報の交換の全体評価を実施する。その全体評価は、目的に照らして達成された結果の検討、基礎となっている正当化事由の有効性が継続していることの評価、中央 SIS との関係におけるこの規則の適用、中央 SIS の安全性、並びに、将来の業務遂行の実装を含める。その評価報告書は、AFIS、及び、第 19 条に従って欧州委員会により実施された SIS 情報提供キャンペーンの評価も含める。

欧州委員会は、欧州議会及び理事会に対し、その評価報告書を提出する。

10. 欧州委員会は、本条第 7 項に示す中央リポジトリの運営に関する細則、並びに、そのリポジトリに適用されるデータ保護規則及びセキュリティ規則を定めるための実装行為を採択する。それらの実装行為は、第 76 条第 2 項に示す審議手続により採択される。

第 75 条 委任の実行

1. 本条に定める条件に服し、欧州委員会に対して、委任される行為を採択する権限が与えられる。
2. 第 38 条第 3 項及び第 43 条第 4 項に示す委任される行為を採択する権限は、2018 年 12 月 27 日から不定期間で、欧州委員会に対して与えられる。
3. 第 38 条第 3 項及び第 43 条第 4 項に示す権限の委任は、いつでも、欧州議会または理事会によって取消され得る。その取消しの決定は、当該決定の中で指定された権限の委任を終了させる。その決定は、EU 官報上でその決定が公示された翌日、または、その決定の中で指定されたその後の日に発効する。その決定は、既に発効している委任される行為の有効性を害してはならない。

4. 委任される行為を採択する前に、欧州委員会は、より良い立法に関する 2016 年 4 月 13 日の機関間合意に定める基本原則に従い、各構成国から指定された専門家と協議する。
5. 委任される行為を欧州委員会が採択した後、直ちに、欧州委員会は、欧州議会及び理事会に対し、そのことを同時に通知する。
6. 第 38 条第 3 項及び第 43 条第 4 項により採択された委任される行為は、当該行為が欧州議会及び理事会に通知された後、2 か月以内に欧州議会及び理事会のいずれからも異議が表明されなかった場合、または、その期間が満了する前に、欧州議会及び理事会の両者が、欧州委員会に対し、異議を述べない旨を通知した場合に限り、発効する。その期間は、欧州議会または理事会の発意により、2 か月まで延長される。

第 76 条 委員会の手続

1. 欧州委員会は、委員会の補佐を受ける。この委員会は、規則(EU) No 182/2011 の意味における委員会である。
2. 本項への参照があるときは、規則(EU) No 182/2011 の第 5 条が適用される。

第 77 条 決定 2007/533/JHA の改正

決定 2007/533/JHA は、以下のとおり、改正される：

(1) 第 6 条は、以下のとおり、置き換えられる：

「**第 6 条 国内システム**

1. 各構成国は、その構成国の N.SIS II の設置、維持管理及び更なる開発並びに N.SIS II の NI.SIS への接続について職責を負う。
2. 各構成国は、SIS II のデータのエンドユーザに対する可用性が途切れないことを確保することについて職責を負う。」；

(2) 第 11 条は、以下のとおり、置き換えられる：

「**第 11 条 機密性－構成国**

1. 各構成国は、国内法に従い、SIS II データ及び補足情報を扱う仕事を要求される全ての個人及び組織に対し、職業上の秘密またはそれ以外の均等な機密保持義務に関するその構成国の規定を適用する。その義務は、それらの者が職場または就業を終えた後、または、それらの組織の活動が終了した後においても、適用される。
2. SIS II と関連する職務において、構成国が外部の契約者と協力する場合、その構成国は、とりわけ、安全性、機密性及びデータ保護に関し、この規則の全ての条項の遵守を確保するため、その契約者の活動を仔細に監視する。
3. 民間会社または民間団体に対して N.SIS II またはその技術複製物の業務運営管理を委託してはならない。」；

(3) 第 15 条は、以下のとおり、改正される：

(a) 以下の項が挿入される：

「3a 運営機関は、CS-SIS の中にあるデータの品質の確認を実施するための仕組み及び手続を開発及び維持管理する。

運営機関は、欧州委員会に対し、直面する問題及び関係する構成国を包摂する定期報告書を提出する。

欧州委員会は、欧州議会及び理事会に対し、直面するデータの品質上の問題に関する定期報告書を提出する。」;

(b) 第 8 項は、以下のとおり、置き換えられる:

「8. SIS II の業務運営管理は、この規則に従い、1 日 24 時間、週 7 日間、SIS II の稼働を維持するために必要となる全ての職務、とりわけ、システムの円滑な作動のために必要となる保守管理作業及び技術開発によって構成される。それらの職務は、第 9 条に定める技術上の遵守の要件に従って SIS II 及び N.SIS II が運用されることを確保する SIS II 及び N.SIS II の試験活動の調整、維持管理及び支援も含める。」;

(4) 第 17 条において、以下の項が挿入される:

「3. SIS II と関連する職務において、運営機関が外部の契約者と協力する場合、その運営機関は、とりわけ、安全性、機密性及びデータ保護に関し、この規則の全ての条項の遵守を確保するため、その契約者の活動を仔細に監視する。

4. 民間会社または民間団体に対して CS-SIS の業務運営管理を委託してはならない。」;

(5) 第 21 項において、以下の項が挿入される:

「個人または対象物がテロリスト行為と関連する警報に基づき求められている場合、その案件は、SIS II 内の警報を保証するために十分に適切であり、関連性があり、かつ、重要であると判断される。公共の安全または国家安全保障を根拠として、構成国は、それが公的調査または法律上の調査、捜査または手続の妨げとなり得るおそれがある場合、例外として、警報を入れることを控えることができる。」;

(6) 第 22 条は、以下のとおり、置き換えられる:

「第 22 条 写真及び指紋の入力、確認または検索のための条件

1. 写真及び指紋は、それらがミニマムの品質基準を満たすか否かを確認するための個別の品質確認の後に限り、入れられる。個別の品質確認の仕様は、第 67 条に示す手続に従って策定される。

2. 写真及び指紋が SIS II 内の警報の中で利用可能な場合、そのような写真及び指紋のデータは、SIS II の中で行われた符号の検索の結果として発見された者の同一性を確認するために使用される。

3. 指紋データは、全ての場合において、個人を識別するために検索され得る。ただし、指紋データは、他の手段によっては個人の同一性が確認され得ない場合において、個人の識別のために検索される。その目的のために、SIS II は、自動指紋識別システム（AFIS）を含める。

4. それらのセットの紋が侵害行為の実行者に属するという高度の蓋然性が確定され得る場合において、かつ、構成国の関連国内指紋データベース内において同時に検索が実施されることを条件として、捜査中の重大犯罪またはテロリスト行為の現場において発見された完全なセットまたは不完全なセットの指紋または掌紋を使用して第 24 条及び第 26 条に従って入れられた警報との関係において SIS II の中にある指紋検証法データも検索され得る。」;

(7) 第 41 条は、以下のとおり、置き換えられる:

「**第 41 条 Europol による SIS II 内のデータへのアクセス**

1. 欧州議会及び理事会の規則(EU) 2016/794(*)によって設置された欧州連合法執行協力局（Europol）は、その任務を果たすために必要があるときは、SIS II の中にあるデータにアクセスし、そのデータを検索する権利をもつ。Europol は、SIRENE マニュアルの条項に従い、補足情報を交換し、かつ、更に要求することもできる。
2. Europol の検索によって、SIS II の中に警報が存在することが明らかとなった場合、Europol は、発行構成国に対し、通信インフラにより、かつ、SIRENE マニュアルに定める条項に従い、補足情報の交換によって、通知する。補足情報の交換のために予定されている機能を Europol が利用可能となるまでの間、Europol は、規則(EU) 2016/794 に定める経路を介して、発行構成国に通知する。
3. Europol は、規則(EU) 2016/794 の第 18 条第 2 項の(a)、(b)及び(c)に示す関係性またはそれ以外の関連性の識別を狙いとし、並びに、戦略分析、主題分析または業務分析のための、補足情報と Europol データベースとの照合及び業務分析プロジェクトの目的のために、構成国から Europol に対して提供された補足情報を処理できる。本条の目的のための補足情報の Europol による処理は、同規則に従って実施される。
4. SIS II 内の検索から得られた情報または補足情報の処理から得られた情報の Europol による利用は、発行構成国の同意に服する。その構成国がそのような情報の利用を許容する場合、その情報の Europol による取扱いは、規則(EU) 2016/794 によって規律される。Europol は、発行構成国の同意があり、かつ、データ保護に関する欧州連合法を全面的に遵守する場合に限り、第三国及び第三者に対し、そのような情報を送付する。
5. Europol は:
   (a) 第 4 項及び第 6 項を妨げることなく、SIS II のいかなる部分とも接続してはならず、Europol がアクセスをもつ SIS II の中に収録されたデータを、Europol によって、または、Europol において運営されるデータの収集及び処理のためのシステムに対して送信してはならず、SIS II のいかなる部分についてもダウンロードまたはそれ以外の複製をしてはならない;
   (b) 規則(EU) 2016/794 の第 31 条第 1 項に拘らず、関連する警報が削除された後、遅くとも 1 年以内に、個人データを含む補足情報を削除する。特例により、Europol がそのデータベース内または業務分析プロジェクト内に、その補足情報と関係する案件に関する情報をもつ場合、Europol がその職務を遂行するため、Europol は、例外として、それが必要なときは、その補足情報を記録保存し続けることができる。Europol は、発行構成国及び執行構成国に対し、そのような補足情報の記録保存を継続することを通知し、かつ、その正当化事由を示す;
   (c) 補足情報を含め、SIS II の中にあるデータへのアクセスを、彼らの職務の遂行のためにそのようなデータへのアクセスを必要とし、個別の承認を受けた Europol 職員に限定する;
   (d) 第 10 条、第 11 条及び第 13 条に従い、セキュリティ、機密性及び自己監視を確保するための措置を採択及び適用する;
   (e) SIS II データを処理することの承認を受けた Europol の職員が、第 14 条に従い、

適切な訓練及び情報提供を受けることを確保する；並びに、

(f) 規則(EU) 2016/794 を妨げることなく、SIS II の中にあるデータへのアクセス及びそのデータを検索するための Europol の権利の行使における Europol の活動、並びに、補足情報の交換及び処理における Europol の活動を、欧州データ保護監督官が監視し、見直しできるようにする。

6. Europol は、適正な承認を受けた Europol 職員が直接の検索を実施するため、そのような複製行為が必要な場合において、技術的な目的のためにのみ、SIS II からのデータを複製する。この規則は、そのような複製物に適用される。技術上の複製物は、それらのデータが検索中において SIS II データを記録保存する目的のためにのみ使用される。データが検索された後、それらの複製物は、削除される。そのような利用は、SIS II データの違法なダウンロード行為または複製行為であると判断されてはならない。Europol は、構成国から発された警報データもしくは追加データ、または、CS-SIS II からの警報データもしくは追加データを Europol の他のシステム内に複製してはならない。

7. データ処理、自己監視の適法性を確認する目的のために、及び、データの適正な安全性及び完全性を確保する目的のために、Europol は、第 12 条の条項に従い、SIS II への全てのアクセス及び SIS II 内の全ての検索の履歴（ログ）を保存する。そのような履歴（ログ）及び文書は、SIS II の一部の違法なダウンロード行為または複製行為であると判断されてはならない。

8. 構成国は、Europol に対し、補足情報の交換によって、テロリスト行為と関連する警報の該当ありを通知する。そのようにすることが、現在進行中の捜査、個人の安全を危険に晒すおそれがあるとき、または、発行構成国の安全上の重要な利益に反するときは、構成国は、例外として、Europol に対して通知しないことが可能である。

9. 第 8 項は、Europol が第 1 項に従って補足情報を取得できる日から適用される。」；

(8) 以下の条が挿入される：

「第 42 条 a 欧州国境沿岸警備チーム、帰国関連の職務に関与する職員のチーム及び移民管理支援チームの構成員による SIS II 内のデータへのアクセス

1. 欧州議会及び理事会の規則(EU) 2016/1624(**)の第 40 条第 8 項に従い、同規則の第 2 条の(8)及び(9)に示すチームの構成員は、彼らの任務の範囲内において、かつ、彼らがこの規則の第 27 条第 1 項に従って検問を実施することの承認を受けており、かつ、この規則の第 14 条に従って必要な訓練を受けたことを条件として、彼らの職務を遂行するために必要な範囲内で、かつ、個別の業務遂行に関する業務遂行計画によって要求されるとおり、SIS II の中にあるデータへアクセスし、そのデータを検索する権利をもつ。SIS II の中にあるデータへのアクセスは、他のいかなるチーム構成員にも拡大されてはならない。

2. 第 1 項に示すチーム構成員は、技術インタフェイスを介して、第 1 項に従った SIS II 内のデータへのアクセス及びそのデータの検索の権利を行使する。その技術インタフェイスは、欧州国境沿岸警備局によって設置及び維持管理され、かつ、中央 SIS II への直接の接続を許容する。

3. 本条第 1 項に示すチーム構成員による検索によって、SIS II 内に警報が存在することが明らかになった場合、発行構成国は、そのことの通知を受ける。規則(EU) 2016/1624 の第 40 条に従い、チームの構成員は、国境警備隊員、または、彼らが業務遂行しているホスト構成国の帰国関連の職務に関与する職員からの指示の下において、かつ、原則として、それらの者が立会する場合に限り、SIS II 内の警報に対応する行動を執る。ホスト構成国は、チーム構成員に対し、その構成国の代わりに行動することを承認できる。

4. データ処理の適法性を確認し、自己監視し、及び、データの安全性及び完全性を確保する目的のために、欧州国境沿岸警備局は、第 12 条の条項に従い、SIS II への全てのアクセス及び SIS II 内の全ての検索の履歴（ログ）を保存する。

5. 欧州国境沿岸警備局は、第 10 条、第 11 条及び第 13 条に従い、セキュリティ、機密性及び自己監視を確保するための措置を採択及び適用し、かつ、本条第 1 項に示すチームがそれらの措置を適用することを確保する。

6. 本条のいかなる条項も、データ保護と関連する規則(EU) 2016/1624 の条項、及び、欧州国境沿岸警備局による違法または不正確なデータ処理に対する欧州国境沿岸警備局の法的責任を損なうように解釈されてはならない。

7. 第 2 項を妨げることなく、SIS II のいかなる部分も、第 1 項に示すチームまたは欧州国境沿岸警備局によって運営されるデータの収集及び処理のためのシステムと接続されてはならず、また、それらのチームがアクセスをもつ SIS II 内のデータをそのようなシステムに移転してはならない。SIS II のいかなる部分も、ダウンロードまたは複製されてはならない。アクセス及び検索を履歴（ログ）記録することは、SIS II データの違法なダウンロード行為または複製行為であると判断されてはならない。

8. 欧州沿岸警備局は、SIS II の中にあるデータへのアクセス及びそのデータの検索のための彼らの権利の行使における本条に示すチームの活動を、欧州データ保護監督官が監視し、見直しできるようにする。このことは、規則(EU) 2018/1725(***)の別の条項を妨げてはならない。

(*) 欧州連合法執行協力局（Europol）の設置に関する、並びに、理事会決定 2009/371/JHA、理事会決定 2009/934/JHA、理事会決定 2009/935/JHA、理事会決定 2009/936/JHA 及び理事会決定 2009/968/JHA を廃止する欧州議会及び理事会の 2016 年 5 月 11 日の規則(EU) 2016/794（OJ L 135, 24.5.2016, p. 53）

(**) 欧州国境沿岸警備に関する、並びに、欧州議会及び理事会の規則(EU) 2016/399 を改正し、欧州議会及び理事会の規則(EC) 863/2007、理事会規則(EC) No 2007/2004 及び理事会決定 2005/267/EC を廃止する欧州議会及び理事会の 2016 年 9 月 14 日の規則(EU) 2016/1624（OJ L 251, 16.9.2016, p. 1）

(***) 欧州連合の機関、組織、事務局及び部局による個人データの処理と関連する自然人の保護及びそのデータの支障のない移動に関する、並びに、規則(EC) No 45/2001 及び決定 No 1247/2002/EC を廃止する欧州議会及び理事会の 2018 年 10 月 23 日の規則(EU) 2018/1725（OJ L 295, 21.11.2018, p.39）」。

第 78 条 廃止

規則(EC) No 1986/2006 並びに決定 2007/533/JHA 及び 2010/261/EU は、第 79 条第 5 項第 1 副項に定めるこの規則の適用の日から、廃止される。

廃止される規則(EC) No 1986/2006 並びに決定 2007/533/JHA への参照は、この規則への参照として解釈され、かつ、別紙の新旧対照表に従って読み替えられる。

第 79 条 発効、業務開始及び適用

1. この規則は、EU 官報上で公示された翌日から 20 日目に発効する。
2. 欧州委員会は、遅くとも 2021 年 12 月 28 日までに、以下の条件に適合していることの確認を経た上で、この規則による SIS の業務開始の日を定める決定を採択する:
   (a) この規則の適用のために必要な実装行為が採択されたこと;
   (b) この規則により SIS データを処理し、補足情報を交換するために必要となる技術上及び法律上の手配を構成国が行ったことを、構成国が、欧州委員会に対し、通知したこと;並びに、
   (c) CS-SIS に関し、及び、CS-SIS と N.SIS との間の相互動作に関し、全ての試験活動が成功裡に完了したことを、eu-LISA が、欧州委員会に対し、通知したこと。
3. 欧州委員会は、第 2 項に定める条件の段階的な充足の過程を仔細に監視し、かつ、欧州議会及び理事会に対し、同項に示す確認の結果に関して通知する。
4. 欧州委員会は、2019 年 12 月 28 日までに、及び、その後は、第 2 項に示す欧州委員会の決定が行われるまでの間、毎年、欧州議会及び理事会に対し、この規則の全面的な実装のために準備の進捗状況に関する報告書を提出する。その報告書は、かかった費用、及び、費用全体に影響を及ぼし得るリスクに関する詳細情報も含める。
5. この規則は、第 2 項に従って決定される日から適用される。
   第 1 副項からの特例により:
   (a) 第 4 条第 4 項、第 5 条、第 8 条第 4 項、第 9 条第 1 項及び第 5 項、第 12 条第 8 項、第 15 条第 7 項、第 19 条、第 20 条第 4 項及び第 5 項、第 26 条第 6 項、第 32 条第 9 項、第 34 条第 3 項、第 36 条第 6 項、第 38 条第 3 項及び第 4 項、第 42 条第 5 項、第 43 条第 4 項、第 54 条第 5 項、第 62 条第 4 項、第 63 条第 6 項、第 74 条第 7 項及び第 10 項、第 75 条、第 76 条、第 77 条の(1)ないし(5)、並びに、本項の第 3 項及び第 4 項は、この規則の発効の日から適用され;
   (b) 第 77 条の(7)及び(8)は、2019 年 12 月 28 日から適用され;
   (c) 第 77 条の(6)は、2020 年 12 月 28 日から適用される。
6. 第 2 項に示す欧州委員会の決定は、EU 官報上で公示される。

この規則は、その全体について拘束力があり、全ての構成国において直接に適用される。

ストラスブールにおいて 2018 年 11 月 4 日に行われた。

欧州議会として	理事会として
議長　A. Tajani	議長　K. Edtstadler

別 紙

新旧対照表

決定 2007/533/JHA	この規則
第 1 条	第 1 条
第 2 条	第 2 条
第 3 条	第 3 条
第 4 条	第 4 条
第 5 条	第 5 条
第 6 条	第 6 条
第 7 条	第 7 条
第 8 条	第 8 条
第 9 条	第 9 条
第 10 条	第 10 条
第 11 条	第 11 条
第 12 条	第 12 条
第 13 条	第 13 条
第 14 条	第 14 条
第 15 条	第 15 条
第 16 条	第 16 条
第 17 条	第 17 条
第 18 条	第 18 条
第 19 条	第 19 条
第 20 条	第 20 条
第 21 条	第 21 条
第 22 条	第 42 条及び第 43 条
第 23 条	第 22 条
—	第 23 条
第 24 条	第 24 条
第 25 条	第 25 条
第 26 条	第 26 条
第 27 条	第 27 条
第 28 条	第 28 条
第 29 条	第 29 条
第 30 条	第 30 条
第 31 条	第 31 条
第 32 条	第 32 条

第 33 条	第 33 条
第 34 条	第 34 条
第 35 条	第 35 条
第 36 条	第 36 条
第 37 条	第 37 条
第 38 条	第 38 条
第 39 条	第 39 条
―	第 40 条
―	第 41 条
第 40 条	第 44 条
―	第 45 条
―	第 46 条
―	第 47 条
第 41 条	第 48 条
第 42 条	第 49 条
―	第 51 条
第 42 条 a	第 50 条
第 43 条	第 52 条
第 44 条	第 53 条
第 45 条	第 54 条
―	第 55 条
第 46 条	第 56 条
第 47 条	第 57 条
第 48 条	第 58 条
第 49 条	第 59 条
―	第 60 条
第 50 条	第 61 条
第 51 条	第 62 条
第 52 条	第 63 条
第 53 条	第 64 条
第 54 条	第 65 条
第 55 条	―
第 56 条	―
第 57 条	第 66 条
第 58 条	第 67 条
第 59 条	第 68 条
第 60 条	第 69 条
第 61 条	第 70 条

第 62 条	第 71 条
第 63 条	―
第 64 条	第 72 条
第 65 条	第 73 条
第 66 条	第 74 条
―	第 75 条
第 67 条	第 76 条
第 68 条	―
―	第 77 条
第 69 条	―
―	第 78 条
第 70 条	―
第 71 条	第 79 条

規則(EC) No 1986/2006	この規則
第 1 条、第 2 条及び第 3 項	第 45 条