国立情報学研究所セキュリティ運用連携サービス利用細則

（平成２９年６月２２日
制　　定）

最近改正　令和２年３月２７日

（趣旨）

第１条　この細則は、国立情報学研究所セキュリティ運用連携サービス利用規程（以下「規程」という。）第５条、第８条、第１６条及び第２９条の規定に基づき、大学共同利用機関法人情報・システム研究機構（以下、「機構」という。）におけるセキュリティ連携運用サービス（以下「本サービス」という。）の運用を円滑に行うために必要な事項を定めることを目的とする。

（用語の定義）

第２条　本細則において用いる用語は、規程において定めた他、以下の各号に定めるところによる。

一　「通信内容」とは検知情報のうちヘッダ情報を除く通信に含まれた情報をいう。

（申請内容）

第３条　参加機関は、申請内容として以下の情報を届け出るものとする。

一　監視するネットワークアドレス

二　通知を受信するための連絡窓口メールアドレス

三　サービスポータルを操作する者の連絡先及びクライアント証明書発行可否

（サービスの内容）

第４条　本サービスの内容は以下のとおりとする。

一　参加機関から届け出られたネットワークアドレス（監視対象ネットワークアドレス）に対するセキュリティサービスの構築及び運用

二　監視対象ネットワークアドレスに対する不正アクセスの検知

三　監視対象ネットワークアドレスを通じて侵入しようとするウィルスの検知

四　監視対象ネットワークアドレスを経由した不正アクセスを検知する機器類の運用

五　検知したサイバー攻撃等の推測情報のうち機構が重要と判断した情報の電子メールによる通知

六　既に通知されたサイバー攻撃に対する、機構で保有する情報とそれに対する一般的

な対処方法の電子メールによる通知

七　サービスポータルによる、所属する参加機関に対する攻撃情報の提供

（監視対象）

第５条　機構は、学術情報ネットワークと外部ネットワークの接続点を通過する通信であって、利用申請に際し、参加機関より提出されたネットワークアドレスを通信元又は通信先とする全てのＩＰ通信を監視対象とする。

２　監視対象とされる通信であっても、本システムに過度の負荷を与え、サービスの維持に支障を来すと機構が判断した場合、監視対象の一部又は全部を一時的に監視対象から除外することができるものとする。

（サービスポータル）

第６条　機構は、本サービスを提供するためサービスポータルを設置する。

２　参加機関は、サービスポータルのログイン資格情報を適切に保護し、ログイン資格情報の危殆化が疑われる場合、速やかに機構に連絡するとともに、パスワードの変更、クライアント証明書の更新等の対応を行う。

３　参加機関は、クライアント証明書について、過去に使用したものを含めて逸失しないように適切に管理する。

４　機構及び参加機関がサービスポータルに対して行った操作履歴の保存期間は最低でも3か月とし、期限を定めての削除は行わない。

（検知情報の取り扱い）

第７条　機構は収集した検知情報について、機構が生成する共通鍵によって通信内容を暗号化したうえで、機構が保有するデータベースに保存する。

２　機構は、参加機関の同意なしに検知情報の参照又は復号を行ってはならないものとする。ただし、本サービスの不具合、障害等に対応するために当該情報の参照又は復号が必要である場合を除く。

３　機構は、本サービスの運用において取得した検知情報を取得した翌月の初日を起算日として最大３か月間を限度とする範囲内で保存するものとし、保存期間経過後は速やかに削除するものとする。ただし、機構と参加機関が合意した場合、保存期間を延長又は短縮することができるものとする。

（共通鍵の暗号化及び復号）

第８条　機構は、共通鍵を各参加機関のクライアント証明書公開鍵で暗号化し、その結果を

保有するデータベースに保存するものとする。

2　機構と参加機関は、参加機関ごとに、一定の期間を単位として共通鍵を設定するものとする。

3　前項にいう「一定の期間」は、参加組織ごとの意見を参考として、機構が定めるものとする。

4　機構は、新たに共通鍵を設定した時点で、それまでに用いていた共通鍵があれば直ちに破棄しなければならないものとする。

5　機構及び参加機関は、通信内容を復号しようとする場合には、復号のための申請を行わなければならないものとする。

6　申請を受けた参加機関は、申請内容を参照した上で閲覧の可否を決定するものとし、閲覧を許可する場合には通信内容の復号に必要となる共通鍵を提示するものとする。当該操作を行うことにより、参加機関は閲覧の許可を受けた機構又は参加機関による当該情報の閲覧操作及び当該操作の記録に同意したものとみなす。

（研究用データ）

第９条　機構は、研究用データとして、以下の情報を作成、提供できるものとする。研究用データの提供先は、国立情報学研究所学術情報ネットワーク運営・連携本部（以下「連携本部」という。）の議を経て国立情報学研究所所長（以下「所長」という。）が別途定め、参加機関へ提示するものとする。

一　本サービスで観測されるトラフィックデータに対して IP アドレス、観測日時等をランダム化処理し、参加機関を特定困難とした検知情報。加工の方法は連携本部の議を経て所長が定め、参加機関に提示する。

二　検知情報に含まれるマルウェア及び当該マルウェアのサンドボックス解析結果。提供するマルウェアの種別は連携本部の議を経て所長が定め、参加機関に提示する。

（サービスの提供時間）

第１０条　機構は、休日を除く午前９時から午後５時までの時間帯で次に掲げるサービスを提供するものとする。

一　通知されたサイバー攻撃に対する、ＮＩＩ－ＳＯＣＳ職員による高度な調査、分析

二　利用申請、終了、担当者変更等に係る手続き

（サービス利用期間）

第１１条　本サービスの利用期間は、参加機関が利用を承認された日から当該年度末日までとする。

２　機構は、参加機関から利用終了の申し出がない場合であって、参加機関が本サービスを継続して利用することが適当であると機構が認める場合に、継続した年度末日まで当該機関の利用期間を自動的に延長するものとする。

（利用の終了及び取り消し）

第１２条　参加機関が本サービスの利用を終了する場合は、機構に対し、別に定める利用終了届を提出しなければならない。この場合、届出に記載された日の翌日から終了の効力が生じるものとする。

２　機構は、サービスを利用しようとする機関が次の各号のいずれかに該当する場合、利用申請を承認しない。また、承認後に判明した場合は、承認を取り消すことができるものとする。

一　ＳＩＮＥＴ加入機関又は接続機関でない場合

二　サービスの目的に適合しない場合

三　利用申請が所定の方法に適合しない場合

四　利用申請の内容に虚偽または重大な誤りがある場合

五　利用規程に違反する恐れがあると判断する相当の理由がある場合

六　その他機構が不適当と判断する相当の理由がある場合

（運用状況の点検）

第１３条　連携本部は、運用状況を年１回以上点検しなければならない。また必要に応じてＮＩＩ－ＳＯＣＳ職員や運用に携わった者に報告を求め、これに基づき指導又は助言を行うことができるものとする。

（審議機関への付議）

第１４条　利用規程や本細則を改廃するときは、連携本部へ付議するものとする。ただし、軽易なものの場合は、省略することができるものとする。

（その他）

第１５条　本細則の運用において必要な情報は、別途、所長が参加機関に通知する。

附　則

この細則は、平成２９年７月１日から実施する。

附　則

１　この細則は、令和元年５月17日から施行し、平成３０年９月１９日から適用する。
２　第８条第３項の「一定の期間」は、１週間とする。

附　則

この細則は、令和元年１１月２７日から実施する。

附　則

この細則は、令和２年４月１日から実施する。