資料５

個人情報保護委員会と
サイバーセキュリティ関係省庁・機関との連携の強化

－連携の仕組み整理と覚書締結－

（案）

令和５年３月15日

個人情報保護委員会
Personal Information Protection Commission

（本資料の内容）

＜背景＞

○　企業等からの機密情報等の窃取を企図したサイバー攻撃が一層複雑化・巧妙化し、攻撃対象も拡大し続けている中、近年、個人情報（※１）の漏えい等の要因としても不正アクセスが特に増加傾向にある。

○　このような傾向を受けて、世界プライバシー会議（GPA）においても、サイバーセキュリティ分野における各国データ保護機関の協力、知見・情報の共有等に向けた決議案が採択されており、先進的な海外のデータ保護機関では、既にサイバーセキュリティ関係機関との連携により対応を強化している。

○　個人情報保護委員会（以下「委員会」という。）においても、「個人情報の保護に関する基本方針」（個情法（※２）第７条①）、「個人データの漏えい等の事案への対応に際しての情報セキュリティ関係機関との連携について」（平成29年５月26日第38回個人情報保護委員会）等にあるとおり、外部からの不正アクセスやランサムウェア等の**サイバー攻撃等による各主体が取り扱う保有個人情報や個人データの漏えい等について、その未然防止や適切かつ迅速な対応による被害の拡大防止等を通じ、プライバシーや財産的な権利利益等の侵害リスクを低減し、個人の権利利益を保護**するため、情報共有等により関係省庁及びサイバーセキュリティ関係機関と緊密に連携する必要がある。

（※１）本資料では、特定個人情報も含めて単に「個人情報」という。
（※２）本資料では、「個人情報の保護に関する法律（平成15年法律第57号）」を「個情法」という。

＜本取組み＞

○　関係省庁及びサイバーセキュリティ関係機関（※１）との連携の仕組み（役割、対応フロー、連携の手法、留意点等）の全体像について、「セキュリティインシデント発生時における連携の在り方」と「平時における連携の在り方」に分けたうえで、より具体的に整理・明確化（※2）・共有することで連携を更に緊密に行っていく。

○　その上で、委員会と同様に報告等（※３）を受ける、内閣官房内閣サイバーセキュリティセンター（NISC）、警察庁サイバー警察局、独立行政法人情報処理推進機構（IPA）については、別添のとおり、覚書を締結し、個別に連携を具体化する。

※1　関係省庁及びサイバーセキュリティ関係機関については、P.7参照

※2　本取組みを通じて、不正アクセスによる個人情報の漏えい等があった場合の既存の報告フロー等を変更するものではない。

※3　委員会　　：個情法第26条第１項及び同法第68条第１項に規定する報告
NISC　　：サイバーセキュリティ基本法第32条に規定する資料又は情報の提供等
警察庁サイバー警察局：都道府県警察への通報
IPA　　：コンピュータウイルス対策基準及びコンピュータ不正アクセス対策基準に規定する届出

（参考）

個人情報の保護に関する基本方針（平成16年４月２日閣議決定、令和４年４月１日一部変更）（抄）

１　個人情報の保護に関する施策の推進に関する基本的な方向

（4）　サイバーセキュリティ対策の取組

　サイバー攻撃の高度化、サイバーセキュリティに関するリテラシーや人材の不足、クラウドサービスの普及、グローバルなサプライチェーンの複雑化、国家の関与が疑われる攻撃等による国家安全保障上への課題に発展する事態の顕在化等のリスクが高まってきている。

　以上のリスクを的確に把握し、サイバー空間における不確実性の制御や不安感の払拭に対応していくことが重要であり、あらゆる個人、分野や地域等において、サイバーセキュリティの確保が必要とされる時代が到来している。このような中、個人情報等の漏えい等のリスクを軽減するためには、各主体の自律的な取組（自助）のみならず、各主体の連携・協力（共助）及びそれらの基盤となる公助を通じた多層的な取組が重要である。

２　国が講ずべき個人情報の保護のための措置に関する事項

（3）　個別事案への対応

② サイバーセキュリティ対策や経済安全保障の観点等からの対応

　サイバーセキュリティ対策の観点から、個人情報保護委員会は、各主体が取り扱う保有個人データや個人データの外部からの不正アクセスやランサムウェア等のサイバー攻撃等による漏えい等の未然防止や被害の拡大防止等のリスク低減、漏えい等事態への適切かつ迅速な対応を図るため、NISC等の関係省庁等及びサイバーセキュリティ関係機関と緊密に連携する。

「個人情報保護法サイバーセキュリティ連携会議」の設置について（抄）

（平成29年５月26日　関係機関・関係省庁申合せ）

１　趣旨

（前略）平成29年５月30日の改正個人情報保護法の施行により、個人情報保護委員会が個人情報取扱事業者等の監督を一元的に行うことから、第38回個人情報保護委員会において、個人情報取扱事業者により外部からの不正アクセス等による個人データの漏えい等の事案への対応が適切に実施されるよう、個人情報保護委員会事務局と情報セキュリティ関係機関との連携を実施することが決定された。

　当該決定を踏まえ、個人情報保護委員会事務局、関係機関及び関係省庁間での円滑かつ効果的な連携及び協力の実施に資するよう、「個人情報保護法サイバーセキュリティ連携会議」を設置するものである。

（本資料の範囲）

＜連携の可能性がある範囲＞

○　委員会と関係省庁・機関の役割等が重複する部分、すなわち、「セキュリティインシデントのうち、電子ファイルに保管された個人情報の漏えい等が発生した場合又は発生のおそれがある場合」が連携の可能性がある範囲となる。

(※)紙帳票、外部電磁記憶媒体の紛失やメールの誤送信など

（ 目 次 ）

Ⅰ　関係省庁・機関の役割・関係性

・ 関係省庁・機関の役割・関係性

（注）関係省庁・機関は、次の会議の構成機関を指す
- 個人情報保護法サイバーセキュリティ連携会議
- 特定個人情報セキュリティ関係省庁等連絡協議会

サイバーセキュリティ関係機関
- （一社）JPCERT コーディネーションセンター
- （独）情報処理推進機構（IPA）セキュリティセンター
- （国研）情報通信研究機構（NICT）サイバーセキュリティ研究所
- （一財）日本サイバー犯罪対策センター（JC３）
- 地方公共団体情報システム機構（J-LIS）

所管等

（インシデント発生時・平時）
調査研究等に基づく知見
その他協力

サイバーセキュリティ関係省庁
- 警察庁サイバー警察局サイバー企画課
- 総務省サイバーセキュリティ統括官室

（インシデント発生時・平時）
調査研究等に基づく知見その他協力

所管等

連携

連携

赤字：連携の在り方を本資料で整理

サイバーセキュリティ関係省庁
- 内閣官房内閣サイバーセキュリティセンター（NISC）（※１）
- 総務省自治行政局デジタル基盤推進室（※2）
- 経済産業省商務情報政策局サイバーセキュリティ課（※3）

連携

個人情報保護委員会　※4

(※1)行政機関等、重要インフラ等のインシデント時に所管省庁経由で報告受領
(※2)地方公共団体のインシデント時に報告受領
(※3)民間事業者のインシデント時に報告受領

(※4)報告は、個人情報取扱機関等から直接受領するほか、権限委任先省庁を経由して受領

（インシデント発生時）
報告

（インシデント発生時）
・事実確認・原因究明、・再発防止策への助言
・注意喚起、権限行使　等

（平時）
・安全管理措置の基準の提示
・教育研修、広報周知、・情報共有　等

（インシデント発生時）
報告

個人情報取扱機関・事業者

国税庁、厚生労働省　等　※5
（システム系部局・個人情報制度所管部局）

(※5)この他、関係機関、関係省庁に含まれないため、当スライドで記載していないが、個人情報を取り扱う民間事業者として、個人情報取扱事業者が存在し、個人情報を取り扱う行政機関等として地方公共団体等が存在する。

Ⅱ　連携の仕組み

＜凡例＞

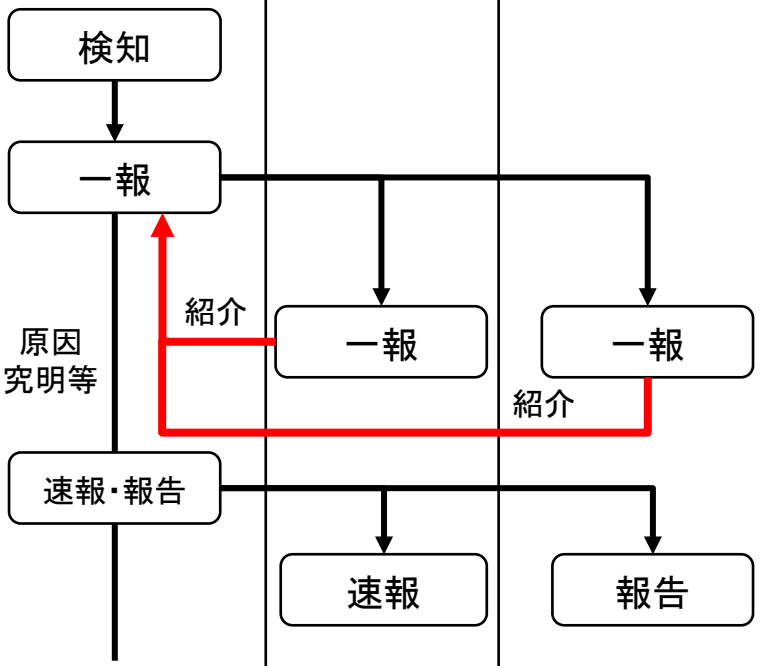
記載上の略称	組織、部局名
NISC	内閣官房内閣サイバーセキュリティセンター
警察	警察庁及び都道府県警察
総務省（デ基）	総務省自治行政局住民制度課デジタル基盤推進室
総務省（CS）	総務省サイバーセキュリティ統括官室
国税庁	国税庁長官官房
厚労省	厚生労働省大臣官房
経産省	経済産業省商務情報政策局サイバーセキュリティ課
JPCERT	（一社）JPCERT/コーディネーションセンター
IPA	（独）情報処理推進機構セキュリティセンター
NICT	（国研）情報通信研究機構サイバーセキュリティ研究所
JC3	（一財）日本サイバー犯罪対策センター
J-LIS	地方公共団体情報システム機構

1．セキュリティインシデント発生時における連携の在り方（概要）

重大インシデント(※1)発生　＜1/3＞

＜連携が想定される主な関係省庁・機関＞

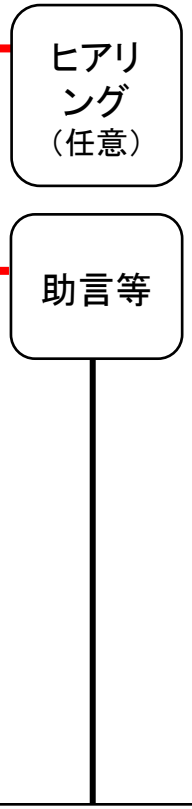
NISC	警察	総務省（デ基）	総務省（CS）	経産省
J-LIS	JPCERT	IPA	NICT	JC3

フェーズ	個人情報取扱機関、事業者等	個人情報保護委員会	関係省庁・機関	連携の在り方
0－1日 事案の検知 3－5日 速報受領				・　関係省庁・機関へ併せて**通報等するよう報告者に紹介** （逆に、関係省庁・機関からも通報者等に対し、委員会へ漏えい等報告が義務付けられていることを紹介）

(※1)個人情報の保護に関する法律施行規則第7条及び第43条、行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の４第１項及び第２項に基づく特定個人情報の漏えい等に関する報告等に関する規則第２条各号に該当する事案をベースとして、当該漏えい等事案における社会的影響の有無や個人情報の漏えい規模などの事案の重大性に照らして判断する。

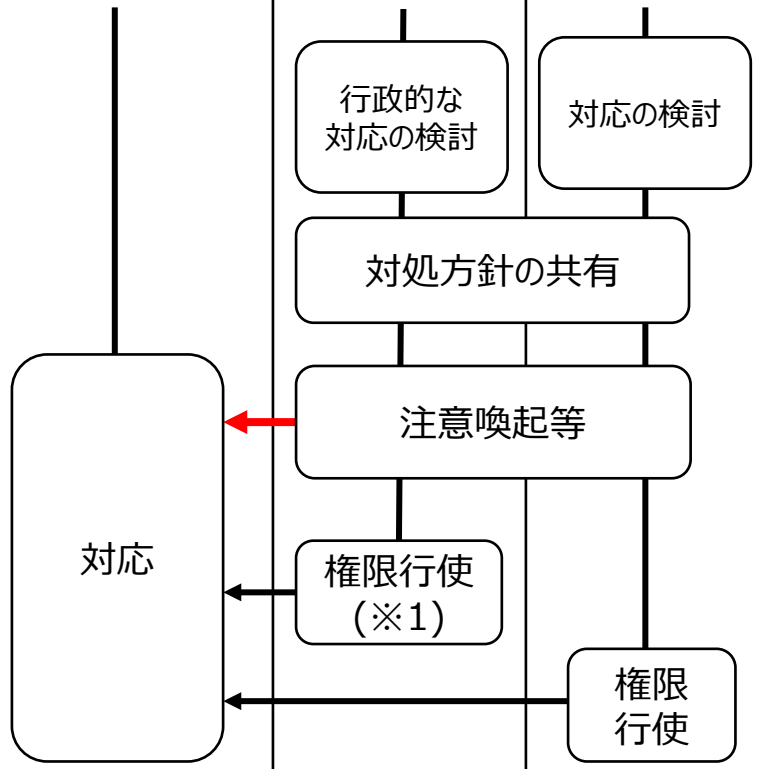
1．セキュリティインシデント発生時における連携の在り方（概要）

重大インシデント発生 <2/3>

フェーズ	個人情報取扱機関、事業者等	個人情報保護委員会	関係省庁・機関	連携の在り方
事実確認等 （原因究明、再発防止策への助言等を含む） **60日以内** **確報受領**				＜事実確認＞ ・ 報告者に対して**任意でのヒアリングを（先方了解を得た上で）共同で**実施、又は、個別にヒアリングを行った場合も可能な範囲で**結果を相互に共有** ⇒ 事実確認の効率化・整合化 ＜原因究明、再発防止策への助言等＞ ・ 各関係省庁・機関における**調査・研究結果による知見、個別事案への技術的助言を踏まえて実施** ⇒ 原因究明等の深度化

1．セキュリティインシデント発生時における連携の在り方（概要）

重大インシデント発生 ＜3/3＞

フェーズ	個人情報取扱機関、事業者等	個人情報保護委員会	関係省庁・機関	連携の在り方
対処 （行政的な対応等を含む）				＜注意喚起・通知等＞ ・ 注意喚起・通知等を発出する際、**連名、相互参照又は「双方調整済み」として実施**する ⇒ 関係省庁・機関による一体的な対応 ＜権限行使等＞ ・ 権限行使等の内容等について、**事前に共有等**した上で実施 ⇒ 関係省庁・機関による一体的な対応

(※1)権限行使は、報告徴取・実地調査・立入検査（個情法第143条、第153条）、指導・助言（個情法第144条、154条）、勧告、命令（個情法第145条、第155条）のいずれか。

2．平時における連携の在り方（概要）

（1）　方針、基準、ガイドライン等における連携

＜連携が想定される主な関係省庁・機関＞

NISC	警察	総務省（デ基）	総務省（CS）	厚労省	国税庁
J-LIS	JPCERT	IPA	NICT	JC3	経産省

- 個人情報の漏えい等の事案への対応に関する各関係省庁・機関が所管する**方針、基準、ガイドライン等における相互参照、取組み等の反映。**
- 上記の方針、基準、ガイドライン等の**内容等に関する整合性等の調整**　等。

（2）　教育・研修における連携

＜連携が想定される主な関係省庁・機関＞

NISC	警察	総務省（デ基）	総務省（CS）	厚労省	国税庁
J-LIS	JPCERT	IPA	NICT	JC3	経産省

- 各関係省庁・機関が保有する教育・研修対象・範囲・ツール等が異なる中、**各関係省庁・機関が行う研修において、相互に場の提供を行うことで**複層的に浸透を図る。
- 研修等内容が類似する場合、**共催研修・共同研修**を実施することで一体的・包括的に浸透を図る。
- 関係省庁・機関による**委員会職員を対象とした研修の実施**、又は、**研修資料の提供**により職員の知見の涵養等を図る（一方、委員会から関係省庁・機関の職員を対象とした研修を実施する、又は、研修資料・参考資料等を提供する）　等。

（注）関係省庁・機関全てにおいて必ず実施することを記載したものではなく、連携の大枠、選択肢を記載するもの。そのため、一部の関係省庁・機関には該当しない場合がある（次スライドも同様）。

2．平時における連携の在り方（概要）

（3） 広報・周知における連携

＜連携が想定される主な関係省庁・機関＞

NISC	警察	総務省（デ基）	総務省（CS）	厚労省	国税庁
J-LIS	JPCERT	IPA	NICT	JC3	経産省

- 各関係省庁・機関等が保有する広報・周知対象・範囲・ツール等が異なる中、**各関係省庁・機関が行う広報・周知において、相互に広報等したい内容を含める**ことで複層的に浸透を図る。
- 広報・周知内容が類似する場合、**共催・共同で周知・広報**を実施することで一体的・包括的に浸透を図る　等。
  （例：報告書、ブログ、ウェブページ（リンクの相互貼付け等）、説明会、シンポジウム、広報誌、ML、チラシ）

（4） 情報共有における連携

＜連携が想定される主な関係省庁・機関＞

NISC	警察	総務省（デ基）	総務省（CS）	厚労省	国税庁
J-LIS	JPCERT	IPA	NICT	JC3	経産省

＜関係省庁・機関　⇒　委員会＞
- セキュリティインシデント（サイバー攻撃、不正アクセス等）に関する**調査・研究結果等を可能な範囲で共有する**ことで、漏えい等事案が起きた場合において委員会が行う原因究明、再発防止策への助言等の深度を深める。

＜委員会　⇒　関係省庁・機関＞
- **特定の個人を識別できないよう加工した個別のセキュリティインシデントの攻撃手法、統計データ、全体的な傾向の共有**により、各関係省庁・機関における調査・研究等の取組みや公表資料等の改訂等の根拠として活用してもらう。

＜情報共有等の場への参画等＞
- 各関係省庁・機関が**既に行っている情報共有の場に参画。**
- **セキュリティインシデント想定訓練**（ケーススタディ）**を共同で実施**　等。

Ⅲ　個別の連携の概要

・個別の連携の概要：セキュリティインシデント発生時

<table>
<tr><th></th><th colspan="2">連携の在り方</th><th>NISC</th><th>警察庁
サイバー警察局</th><th>IPA</th></tr>
<tr><td rowspan="2">セキュリティインシデント発生時</td><td>事案の検知時における連携</td><td>・関係省庁・機関へ併せて通報等するよう報告者に紹介</td><td colspan="3">○報告等の制度の相互紹介
一方が報告等を受けた場合、他方の報告等に関する制度について、当該報告等を行った者に紹介する
（警察庁サイバー警察局は、都道府県警に対し、その旨指導する）</td></tr>
<tr><td>事実確認等・対処における連携</td><td>・共同ヒアリング、ヒアリング結果の相互共有等による事実確認の効率化・整合化
・調査・研究結果による知見、個別事案への技術的助言を踏まえた原因究明・再発防止策への助言等の深度化
・注意喚起・通知等の連名等での実施、権限行使の内容等の事前共有による一体的な対応　等</td><td colspan="3">双方は、一定の留保をつけた上で、
○共同ヒアリング等
○ヒアリング等結果の相互共有
○権限行使の内容等の事前の相互共有
○海外の関係機関の協力により得られた情報の相互共有
○連名での注意喚起
を実施する

○NISC・警察庁サイバー警察局・IPAは、委員会の求めに応じて、報告等を行った者がとるべき初動対応、被害拡大防止、事実関係の調査、原因究明及び再発防止策の検討並びに委員会による注意喚起の発出等に資する技術的な助言を行う等の可能な支援を行う。</td></tr>
</table>

・個別の連携の概要：平時

<table>
<tr><th></th><th colspan="2">連携の在り方</th><th>NISC</th><th>警察庁
サイバー警察局</th><th>IPA</th></tr>
<tr><td rowspan="4">平時</td><td>方針、基準、ガイドライン等における連携</td><td>・相互参照、取組み等の反映
・内容等に関する整合性等の調整等</td><td>○双方は、それぞれが策定する基本方針、統一基準、ガイドライン等（以下「一般基準等」という。）の記載に関する助言や情報等を策定者の求めに応じて提供する。
○双方は、必要に応じて、一般基準等において他方の一般基準等を参照すべきことや他方の業務に言及する等、国の機関として一体的・整合的な施策を公に示すよう努める。</td><td>○警察庁サイバー局は、委員会が策定する基本方針、ガイドライン等の記載に関する技術的な助言や情報等を委員会の求めに応じて可能な範囲で提供する。</td><td>○双方は、それぞれが策定する基本方針、基準、ガイドライン等（以下「一般基準等」という。）の記載に関する助言や情報等を策定者の求めに応じて提供する。
○双方は、必要に応じて、一般基準等において他方の一般基準等を参照すべきことや他方の業務に言及する等、公的機関として整合的な基準を公に示すよう互いに協力する。</td></tr>
<tr><td>教育・研修における連携</td><td>・相互のチャンネルの活用、共同での教育・研修　等</td><td colspan="3">○必要に応じ、双方の取組の活用、共催・共同で教育・研修を実施等する。</td></tr>
<tr><td>広報・周知における連携</td><td>・相互のチャンネルの活用、共同での広報・周知　等</td><td colspan="3">○必要に応じ、双方の取組の活用、共催・共同で広報・周知を実施等する。</td></tr>
<tr><td>情報共有における連携</td><td>・調査・研究結果、統計的データ等の共有
・個別のインシデントの手口等の共有　等</td><td colspan="3">○委員会は、NISC・警察庁サイバー警察局・IPAに対し、頻発する攻撃手法等や統計化された漏えい等の発生状況等を共有する。
○NISC・警察庁サイバー警察局・IPAは、委員会に対し、セキュリティインシデントに関する調査・研究の結果、最新の脅威情報・技術動向等を（可能な範囲で）共有する。</td></tr>
</table>