文書番号：20161130-00

次世代ネットワーク型監視カメラのプライバシー保護研究専門委員会議事録	
会議名	第5回 次世代ネットワーク型監視カメラのプライバシー保護研究専門委員会
日程 場所	2016年10月25日（火）16:00～18:15 産業技術大学院大学265会議室
出席者 （敬称略）	計17名
議題	1. アジェンダおよび議事録確認 2. EU一般データ保護規則 3. 個人情報保護法に関する政令ほか 4. 国際標準化動向改訂（資料の配布のみ） 5. マルチステークホルダー分析改訂（資料の配布のみ） 6. PIA実施（システムリスク分析） 7. PIA実施（業務フローリスク分析） 8. カメラリスク分析 9. 次回の予定
配布資料	20161025-01　第４回議事録 20161025-02　開催通知およびアジェンダ（第五回研究会資料） 20161025-03　監視カメラ（use of biometrics in Video surveillance systems）の国際標準の開発状況（配布のみ） 20161025-04,05　ＥＵ一般データ保護規則とデータ保護影響評価 20161025-06　マルチステークホルダープロセスにおけるプライバシー影響評価の考察（配布のみ） 20161025-07　オリンピックのセキュリティ（配布のみ） 20161025-08,09　リスク分析（システム、データフロー）Ver.1.0 20161025-10　カメラガイドラインリスク分析Ver.0.5 20161025-11　個人情報保護法改訂（８月の意見公募の結果） 20161025-12　危機管理産業展（RISCON TOKYO）2016

No	議事詳細
1	議事録およびスケジュール ・ 9月の議事録は承認された。もし修正が必要であれば、本日中に連絡願う（瀬戸）
2	マルチステークホルダープロセスにおけるプライバシー影響評価の考察（浦田） ・配布資料はCSSで発表した内容を報告書としてまとめてもの。 ・MSPの合意形成のルールはあるのか（委員） →ルールはないが、事例では参加したいステークホルダーは誰でも参加できる。ステークホルダーのグループの代表者が出席する場合もある。自分の意見ばかり主張されたり、強い意見のかい離があると合意形成は難しい。皆が勉強するというスタンスが重要であり難しいところである。（浦田） →成功させるためには、そういった場であることを強調することがポイントだと感じた（委員）
3	危機管理産業展（瀬戸） ・１０月２１日に危機管理産業展において、昨年度の活動をベースとしたものを発表した。

文書番号：20161130-00

4	オリンピックのセキュリティについて ・「オリンピックのセキュリティ」の解説があった。参考に配布資料として配布する（瀬戸）
5	国際標準について（瀬戸） ・前回、9 月に紹介したスライドから、一部修正した。詳細については深い理解には至っていない。詳細わかり次第報告予定（瀬戸）
6	EU 一般データ保護規則（瀬戸） ・報告書は英語版のドキュメントをまとめたものである。配布資料を参照。 ・EU 一般データ保護規則で定められているデータ保護影響評価を中心紹介した。 ・検索ダウンロードしたデータを域外に出してしまった場合はアウトか（委員） →アウト（瀬戸） →日本の携帯事業者は SIM カードの情報を収集している（委員） →アウトである（瀬戸） →日本でＨＰを作成しＥＵのものが閲覧、痕跡が残る場合はセーフ、データ解析等で利用する場合はアウト（瀬戸） ・EU 圏にグループ企業がある場合、検索すると個人情報（所属等）が簡単に集められる。こういったケースも EU データ保護規制に該当するのか？（委員）→該当する。ただし、法律の専門家の見解が必要で、情報が出次第紹介する。（瀬戸）
7	法令調査（個人情報保護法に関する政令ほか） 本委員会に関連すると思われる内容について、説明をおこなった。（白石） 顔認証と顔認識の言葉が 2 つある。顔認証とはログイン等に利用するものであり、認証、認識、識別は意味が違うのではないか。 →　一般の人は区別をしていない。専門家だけでしょう。（瀬戸） 防犯目的であれば社会通念上、防犯カメラ作動中の表示は必要であるが、顔認証システムが稼働している旨を表示することについては言明していない。（委員） →社会通念上みとめられるのは顔識別する手前までではないか（委員） →「参考にさせていただきます」となっているので、ガイドラインは変わっていくのではないか（瀬戸） ・一般市民の感覚では賛否両論、法律で明確にはなっていない。このような場合に PIA は有効になってくるのではないか。（委員） ・第三者提供の一部の例外とは生命、財産と思われるが、万引き犯の顔を登録し他の店舗と共有する場合は、財産を守るための解釈になるのか（委員） →その場合でも同意は必要ではないか（委員） →生命、財産に該当するケースを明確にすべきではないか。（委員） ・犯人として捕まえて、同意しなければ通報するとした場合に同意といえるのか。（委員） ・顔認証に関しては、グレーのままでは済まされないという印象をうけた。（委員） →明確にせず自主的な規定等でもって対策していることを証明する形でもいいのでは（委員）
8	ネットワークカメラシステムにおけるリスク分析（白石） ・非形式アプローチを用いて、脅威を洗い出した。

文書番号：20161130-00

	・カメラシステムの分類ごとに分析を行った内容を紹介した。 ・クラウドに対するリスク対策について →事業者によっては機密保持契約を結びながら、蓄積したデータについてはクラウド事業者が利用している場合がある（クラウド事業者の研究開発のため）。そのため、単純に秘密保持契約を結ぶだけがリスク対策になるかは疑問である（委員） →外部から悪意のあるものがクラウドに侵入する場合、外部からの DDoS 等により、NW 機器やサーバ等の処理を遅延させて情報を搾取する攻撃もある。そのため、事業者の悪意以外にも想定した文言にすれば、適用範囲が広くなるのではないか（委員） →国内に置かれたクラウドサービスの場合、欧州で差し押さえがないことはない。クラウドサービス事業者はデータの所在を公表しない場合が殆どである（委員） →欧州にサーバがあり、まったく関係のない犯罪捜査でサーバが停止してしまった事例もあるので、ドメスティックなクラウドを利用することを前提とする場合もある。 →ただし海外にサーバがおかれている場合ではコストが下がることもあり、リスクを取りながらサービスを利用するケースもある。（委員） →　悪意をもった人がクラウドサーバーを攻撃するというリスクがある。（委員） →　ローカル監視は小さな商店などいう表現あったが、これが一番多い。ローカル監視構成といえるか微妙だが、商店街でも導入されている（委員） →クラウド構成は非常に安価であるため、個人の家などで利用されており、今後も増加すると思われる（委員）
9	システムリスク分析（田） システムリスクに関して、非形式およびベースラインアプローチ（医療 PIA を参考）により分析した結果を説明した。 ・特記すべき内容として →アタッカーはネットワークカメラのアクセスコードを不正に入手し、撮影映像を入手し、漏洩されるリスクがある(田) ・時刻同期(NTP) のズレに関するリスクが考えられる。実際に大阪で防犯カメラの時刻がずれていて誤認逮捕したケースがある（委員） →リスクとして追加するか検討したい（白石、田） ・センター管理者のリスクは教育によって軽減されるということか（委員） →その認識である（白石） →悪意を持った管理者の場合い、必ずしも教育だけでは対策として不十分である（委員） →現在のセンターでは、監視カメラが配置されている（委員） →大日本印刷で起きた情報漏洩の件でも、事件後にカメラが配置されたと新聞報道があった。カメラによる監視も対策になるのではないか（委員）
10	データフローリスク分析（下村） ・ データーフローリスクは非形式およびベースラインアプローチ（日防設のものを参考（により分析を行った結果を説明した。データーフローは 6 つのケースによって実施した。 ・ PIA のリスク分析は 2 つの観点で実施する。一つは設計書に記載されたシステム構成に対し、ハード、ソフトウエアの観点でリスク分析をする。もう一つは、仮想的にシステムを動かし、データの取得から処理管理破棄のライフサイクルでシステムのリスク分析する。つまり業務フローを明確にし、フロー上でのリスクを分析する。（瀬戸）

文書番号：20161130-00

	・ルールなどの不備はリスク分析から明確になるのか（委員） →影響評価で明確になる。システム、データフロー分析ではルールの評価はできない。（瀬戸）
11	その他 ・リオオリンピックで顔認証、監視カメラシステムを運用した企業の方、話題提供頂きたく（瀬戸） ・次年度　具体的なサイトでの評価を実施したい。企業の方に提案願いたい。情報公開の方法は配慮する。（瀬戸） →既に構築されたシステムに対してでも問題ないか（委員） →問題ないが、企画・設計段階が最適である（瀬戸）
12	次回の委員会予定（瀬戸） 日時：11 月 30 日（水）16:00～18:00 場所：産業技術大学院大学 会議室 議題案：仮想システムへの影響評価結果、継続調査報告などを行う。 以　上