Vol.2015-EIP-68 No.10
2015/5/29

# プライバシーに配慮したアプリケーションログ出力の設計

石田 茂[†1]

アプリケーションが出力するログは，運用およびセキュリティの上で重要なものであり，一般にログの取得は要件にもなっている．ログに秘密情報が含まれる場合は，漏洩することによって悪用されるリスクがあり，また個人情報が含まれる場合には，漏洩した際に，当該本人のプライバシーを侵害するリスクがある．よって，ログ出力の指針として，ログに出力する個人情報は必要最小限とすべきであり，出力する情報については，プライバシーへの配慮という観点から，プライバシーリスクを低減する措置をとることが望ましい．本発表では，ログに出力する項目のプライバシーへの影響度を評価して，出力する情報を限定することにより，プライバシーリスクを低減する指針を提案するとともに，現在国会で審議されている個人情報保護法改正案における「匿名加工情報」との関連について考察を述べる．

# Design of the application log output in consideration for privacy

SHIGERU ISHIDA[†1]

The log that application outputs is important on operation and security. Generally, the acquisition of the log also becomes the requirements.When secret information is included in log, a risk exits of being abused by leaking out. When personal information is included in log, a risk exits of infringing the privacy of the person concerned by leaking out.
In Short, it should be said that the personal information to output in log is minimum , and it is desirable to take the measures that the information to output reduces a privacy risk from a point of view called the consideration to privacy,as a guidance of the log output.This presentaion suggests a guidance to reduce a privacy risk by evaluating an influence on privacy degree of the item to output, and limiting information to output to log and consider connection with "the anonymity processing information" in a personal information revision bill discussed now in the Diet.

## 1. はじめに

アプリケーションが出力するログは，運用およびセキュリティの上で重要なものであり，ログの取得を，セキュリティ上の要求事項として定めているガイドラインもある．例えば，個人情報法保護法の経済産業省ガイドライン[1]では，技術的安全管理措置として講じなければならない事項として，「個人データのアクセス記録」をあげている．クレジットカード業界のデータセキュリティ基準であるPCI-DSS[2]では，要件として，「ネットワークリソースおよびカード会員データのすべてのアクセスを追跡および監視する」が要求されている．

ログに秘密情報が含まれる場合には，漏洩することによって悪用されるリスクがある．現実に，ログに含まれる情報を悪用し，銀行のキャッシュカードを偽造し，不正に預金が引出される事案が発生している[3][a].

ログの取得は先に述べたとおり，セキュリティ要件および運用要件,法的あるいは制度上の要求事項となっている．ログは，アプリケーションの運用監視および障害発生時のサポートに利用され，障害の修正(デバッグ)の際に，ログに出力された内容とデータベースに保存された内容を照合することにより，問題箇所を突き止める際に有用である．通常，アプリケーションの開発時と運用時では，ログの出力レベルを切り替え，開発時は詳細な内容を出力し，運用時は出力を抑止する方法が取られるが，再現性のない障害が発生した場合における調査の際には，一定期間，詳細な内容をログに出力することもある．アプリケーションが扱うデータの種類によっては，個人情報や機微性の高い情報もある．

個人情報取扱事業者がベンダーにシステムの運用保守を委託する場合，委託元と委託先との間で秘密保持契約を締結することが条件となるが，委託先からの情報漏えいのリスクはある．また，システムのサポートに必要な情報の中に機微性の高い情報が含まれ，必要以上の範囲の情報が第三者の目に触れることは好ましくはないであろう．よって，ログに出力される個人情報は必要最小限とすべきであり，出力する情報については，本人へのプライバシーへの配慮という観点から，プライバシーリスクを低減する措置をとることが望ましいと言える．

本稿では，ログの出力要件を整理し，国際的な潮流となっているプライバシーに配慮した設計思想の概要を触れ，プライバシーに配慮したアプリケーションログの出力指針を提案する．また，考察として現在国会で審議されている個人情報法の改正案[6]における「匿名加工情報」と本指針によって出力されたログとの関連についても言及する．

†1 情報セキュリティ大学院大学
Institute of Information Security

a)横浜銀行の現金自動預払機(ATM)利用者のデータを不正取得し，偽造したカードで現金を引き出したとして，「支払用カード電磁的記録不正作出」および「不正電磁的記録カード所持」などの罪に問われた富士通フロンテック元社員に，横浜地裁は 2014 年 11 月 25 日，懲役 7 年の判決を言い渡した．

## 2. ログ出力の要件

ログはシステム監査や事故調査の際に必要な資料であり，ログの取得をセキュリティ上の要求事項として定めているガイドラインもある．以下に代表的なガイドラインの中からログ出力の要件を記す．

### 2.1 ISO/IEC 27001:2013 および ISO/IEC27002:2013

情報セキュリティマネジメントシステム(Information Management System:ISMS)の認証規格である ISO/IEC 27001:2013(JIS Q 27001:2014)の付属書 A「A.12.4 ログ取得及び監視」において，「イベントログ取得」，「ログ情報の保護」の管理策の実装が要求されている[7]．また，情報セキュリティ管理策の実践のための規範である ISO/IEC 27002:2013(JIS Q 27002:2014)には，実施の手引が記載されている[8]．ISO/IEC 27002:2013(JIS Q 27002:2014)では，「ログ取得及び監視」の目的を「イベントを記録し，証拠を作成するため」とし，「イベントログ取得」の管理策として，「利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューすることが望ましい」としている．実施の手引として，以下の事項をイベントログに含めることが望ましいとしている．

a)利用者 ID
b)システムの動作
c)主要なイベントの日時及び内容（例えば，ログオン，ログオフ）
d)装置の ID 又は所在地（可能な場合），及びシステムの識別子
e)システムへのアクセスの，成功及び失敗した試みの記録
f)データ及び他の資源へのアクセスの，成功及び失敗した試みの記録
g)システム構成の変更
h)特権の利用
i)システムユーティリティ及びアプリケーションの利用
j)アクセスされたファイル及びアクセスの種類
k)ネットワークアドレス及びプロトコル
l)アクセス制御システムが発した警報
m)保護システム（例えば，ウィルス対策システム，侵入検知システム）の作動及び停止
n)アプリケーションにおいて利用者が実行したトランザクションの記録

さらに，「イベントログには，取扱いに慎重を要するデータ及び PII (Personally Identifiable Information:PII) が含まれる場合がある．適切なプライバシー保護対策をとることが望ましい」と記されている．

### 2.2 PCI-DSS

PCI-DSS では，「要件 10:ネットワークリソースおよびカード会員データのすべてのアクセスを追跡および監視する」において，監査可能なイベントに対して，下記の内容を含む詳細を記録することを要求している．

10.3 イベントごとに，すべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録する
10.3.1 ユーザ識別
10.3.2 イベントの種類
10.3.3 日付と時刻
10.3.4 成功または失敗を示す情報
10.3.5 イベントの発生元
10.3.6 影響を受けるデータ，システムコンポーネント，またはリソースの ID または名前

なお，PCI-DSS では，「要件 3: 保存されるカード会員データを保護する」において，カード会員データを，暗号化，トランケーション，マスキング，ハッシュなどの方式によって保護することを要求している．

### 2.3 地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）

「地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション）」[9]は，地方公共団体において Web アプリケーションを導入するにあたり，システムの脆弱性をなくし，安全に運用するために必要な要求仕様事項を取りまとめた特記仕様書の例である．同仕様にて，「4.5. ログ出力」として要件が定義されていおり，アプリケーションログで取得するイベントとして以下をあげている．

(1)ログイン(成功・失敗問わず)
(2)ログアウト
(3)アカウントロック
(4)利用者登録・登録削除
(5)利用者の登録内容更新
(6)利用者のパスワード変更
(7)秘密情報の参照
(8)その他重要な操作

また出力するログの項目として以下をあげている．

(1)アクセス日時
(2)アクセス元 IP アドレス
(3)利用者 ID
(4)アクセス対象
(5)操作内容

(6)操作対象
(7)実行結果(成功あるいは失敗，処理件数等)

また，出力しないログの項目として，「パスワード」をあげ，ログからの情報漏えい・改ざん対策として，以下をあげている．

(1) ログが不正に参照・変更・削除されないよう保護すること
(2) ログから個人情報等の秘密情報が漏えいすることを防ぐため，ログの目的(監査，事故追跡)を損なわない範囲で秘密情報を含めない処理または秘密情報の一部のみの出力(マスク処理)をすること．

## 3. プライバシー保護のための設計思想

ICT 技術の進展の伴い，電子化された個人情報の蓄積・利活用が進み，利便性が向上する一方で，個人情報の目的外使用や漏えい等によるプライバシー侵害のリスクが増えている．そこで，近年，プライバシー保護のための設計思想であるプライバシー・バイ・デザイン[10]が注目されている．

### 3.1 プライバシー・バイ・デザイン

プライバシー・バイ・デザイン(Privacy by Design:PbD）とは，直訳すれば，「デザイン(設計)に基づくプライバシー」となるが，「プライバシー情報を扱うあらゆる側面においてプライバシー情報が適切に取り扱われる環境をあらかじめ作り込もうというコンセプト」である．カナダ・オンタリオ州の情報・プライバシー・コミッショナー，アン・カブキアン博士よって 1990 年代半ばに提唱された．

PbD の核となるのは以下の 7 つの基本原則である．

(1)事後的でなく事前的，救済策でなく，予防的であること
プライバシー侵害が発生する前に，それを予想し予防するを目的とする．

(2)プライバシー保護は初期設定で有効化されていること
プライバシー保護の仕組みはシステムの最初から組み込まれ，利用者のプライバシーは利用者が特に何もしなくても，保護されるようにする．

(3)プライバシー保護の仕組みがシステム構造に組み込まれること
プライバシー保護の仕組みは，IT システムおよびビジネス慣行のデザインおよび構造に組み込まれるものである．事後的に，付加機能として追加するものではない．

(4)ゼロサムではなくポジティブ
サムプライバシー保護の仕組みを設けることによって，利便性を損なうなどトレードオフの関係を作ってしまうゼロサムアプローチではなく，すべての正当な利益および目標をもたらすポジティブサムを目指す．

(5)データはライフサイクル全般にわたって保護されること
個人情報を含むデータは，生成される段階から廃棄される段階まで，常に強固なセキュリティで守られなければならない．

(6)プライバシー保護の仕組みと運用は可視化され透明性が確保されること
どのようなビジネス慣行または技術が関係しようとも，プライバシー保護の仕組みが機能することを，すべての関係者に保証する．この際，システムの構成および機能は，利用者および提供者に一様に，可視化され，検証できるようにする．

(7)利用者のプライバシーを最大限に尊重する
利用者個人が自らプライバシー保護を簡単に実現できるオプション手段を提供し，利用者個人の利益を最大限に維持する．

プライバシー・バイ・デザインは，EU のデータ保護規則案[11]，米国の FTC レポート[12]，国内では総務省が取りまとめたスマートフォン・プライバシー・イニシアティブ[13]等，各国の政策検討の際に参照され，プライバシー保護施策のグローバル・スタンダードとなりつつある．

### 3.2 プライバシー影響評価およびプライバシー保護強化技術

PbD の実現のためには，プライバシー影響評価(Privacy Impact Assessment:PIA)の実施と技術面の検討が必要である．

PIA とは，情報システム稼働に伴うプライバシーへの影響を事前に評価する手法である．プロセスとしては，評価基準を作成，影響分析を実施，その結果をシステム設計に反映し，プライバシー問題の解決を図るという一連の手順である．PIA を実施することにより，システム稼動後のプライバシーリスクを最小限に抑え，脆弱性の改修に伴う費用の発生を予防し，稼働停止などのビジネスリスクを軽減することができる効果がある．諸外国の中には，行政情報システムの構築にあたり PIA が実施されている国もある[?]．我が国でも，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（平成 25 年法律第 27 号，以下，「番号法」という）において，PIA が導入された．ただし，番号法の PIA は「特定個人情報保護評価」といい，マイナンバー制度の特定個人情報を取扱う事務を実施する機関のみが対象となっている．

また，技術面の検討では，プライバシー保護強化技術(Privacy Enhancing Technology:PETs)の利用を検討する．PETs とは，プライバシー保護を向上させるための技術の総称であり，PETs は，基本的なプライバシー原則(個人情報の利用の最小化，データセキュリティの最大化，個人への権限の付与)を具体化するものである．これらは，例えば，

「データベースに保存する個人情報を暗号化」や「個人情報が含まれるデータを匿名化」等により実現できる．

## 4. プライバシーに配慮したアプリケーションログ出力指針の提案

**アプリケーションログに出力する際に，どの項目は出力しても良いのか，出力時にプライバシーを保護するためにはどのような処置が必要なのか，アプリケーション開発者がプログラミングする上で何らかの指針が必要である．そこで，ログに出力する項目のプライバシーへの影響度を評価し，出力の可否および情報の加工を判断する指針を提案する．**

### 4.1 プライバシーへの影響度の評価

**個人情報を扱うアプリケーションにおいて，どのような情報を保護の対象とするか一般的な基準がない．そこで，出力する情報がプライバシーへ与える影響を評価することに着目した．**

**個人情報のプライバシーへの影響を評価する先行研究としては，NPO 日本ネットワークセキュリティ協会の JO モデルがある[15]．JO モデルは，個人情報漏えいにおける想定損害賠償額の算出モデルであり，想定損害賠償額は，図 1 の式により算出される．**

損害賠償額 ＝ 漏えい個人情報価値
× 社会的責任度
× 事後対応評価

図 1 想定損害賠償額算出モデル

漏えい個人情報の価値は，「精神的苦痛」と「経済的損失」をそれぞれ x 軸 y 軸とする，情報の種類をプロットしたシンプル EP 図(Economic-Privacy Map)(図 2)を参照し，漏えいした情報の価値を推定する．その際，実被害への結びつきやすさを考慮し推定値を補正している．

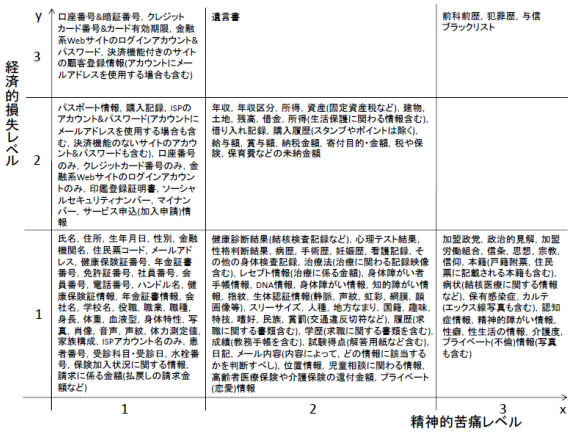


図 2 シンプル EP 図

本稿で提案する指針は，情報の種類を「個人特定性」と「機微性」の 2 軸で評価している．本指針では，被害の金額や損害賠償額の算出は目的としておらず，影響度の度合いの評価を目的とするため，JO モデルに比べ簡易的なものになっている．本指針は，氏名，身長，電話番号などの情報を，「個人を識別する情報」，「身体的特徴の情報」，「物理的なコンタクト情報」などの個人情報カテゴリに分類しており，カテゴリ毎に「個人特定性」と「機微性」から「プライバシーへの影響度」を評価している．「個人特定性」および「機微性」はそれぞれ「高」「中」「低」で評価している．「個人特定性」は「氏名」，「住所」など，実世界において特定の個人を識別する情報や「電話番号」や「E メールアドレス」など実世界やインターネットにおいて個人と連絡をとったり，個人の所在を突きとめたりできるような情報を「高」としている．「機微性」は一般の感受性を基準にして，秘匿したいかどうかを基準としている．例えば，氏名や住所などは「実世界において特定の個人を識別する情報」であり，一般に公開される情報であるため「機微性」は「低」としているが，パスワード等の秘密情報や生体認証情報は機密情報であるため「機微性」は「高」とし，個人の財産に関する情報や通信履歴なども，他人に知られたくない情報であるため，「機微性」を「高」としている．また，法令等で配慮が求められる機微な情報についても，「機微性」を「高」としている．なお，「Web 上の行動履歴」，「購買履歴」，「交通機関等のサービスの利用履歴」は「機微性」を「中」としている．

本指針では，プライバシーへの影響度は，「個人特定性」と「機微性」で評価するが，評価式は図 3 の式を採用している．

プライバシーへの影響度 ＝ max(個人特定性, 機微性)

図 3 プライバシーへの影響度の評価式

評価にあたり，個人特定性が「高」で機微性が「低」の場合でも，影響度は「高」となる．ここでいう影響度には，他人に知られたくないという精神的苦痛だけでなく，本人が特定される容易性も含んでいる．本指針では，影響度を踏まえ，保護方法を例示している．保護方法は，「①出力しない，②マスク処理をおこなう，③識別性を維持するする必要がある場合は一方向ハッシュ関数を使用し符号化する，④出力時に情報の加工は必要としない」からなる．指針の抜粋を図 4 に示す．

| | 個人情報カテゴリ | カテゴリの説明 | カテゴリに含まれる個人情報 | 個人特定性(X) | 機微性(Y) | 影響度(MAX(X,Y)) | 保護方法の例 |
|---|---|---|---|---|---|---|---|
| 1 | 個人を識別する情報 | 実世界において特定の個人を識別する情報 | 氏名、住所、生年月日 | 高 | 低 | 高 | 氏名、住所、生年月日をマスク処理する。 |
| 2 | 身体的特徴の情報 | 個人を特定する身体的特徴の情報 | 身長、体重、体型、その他身体的特徴、写真、ビデオ | 高 | 低 | 高 | 身長、体重、体型、その他身体的特徴をマスク処理する。写真、ビデオは出力しない。 |
| 3 | 物理的なコンタクト情報 | 実世界において個人と連絡をとったり、個人の所在を突きとめたりできるような情報 | 住所、電話番号、FAX番号、携帯電話番号、勤務先、送付先、請求先など | 高 | 低 | 高 | 住所、電話番号、FAX番号、携帯電話番号、勤務先、送付先、請求先などをマスク処理する。 |
| 4 | オンラインのコンタクト情報 | インターネット上で個人と連絡をとったり、インターネット上の所在を突きとめたりできるような情報 | Eメールアドレス、SNSのID、ホームページURLなど | 高 | 低 | 高 | Eメールアドレス、SNSのID、ホームページURLなどをマスク処理をする。 |
| 5 | ユニークなID情報 | 個人を整合的に識別するために発行されたID番号(金融ID番号を除く) | Webサイトの利用者ID、社員番号、顧客番号、会員番号、免許証番号、パスポート番号など | 中 | 中 | 中 | ID、番号はマスク処理する。識別性を維持する場合は、一方向性ハッシュ関数等を使用して符号化し、元の値を復元できないようにする。 |
| 6 | 金融ID情報 | 個人と金融機関、口座、または支払いシステムとを結びつけるID番号 | クレジットカード番号、銀行口座番号など | 中 | 中 | 中 | ID、番号はマスク処理する。 |
| 7 | 秘密情報 | 個人が管理するパスワードや暗証番号などの秘密情報 | パスワード、暗証番号 | 低 | 高 | 高 | 出力しない。 |
| 8 | デバイス情報 | 個人がネットワークにアクセスする時に使用しているデバイスやコンピュータシステムに関する情報 | IPアドレス、ドメイン名、携帯ID、ブラウザの種類、OSの種類など | 中 | 低 | 中 | IPアドレス、ドメイン名、携帯IDはマスク処理する。 |
| 9 | 人口統計学的情報 | 人口統計学的情報において個人を特徴づけるような情報 | 性別、年齢、婚姻、家族構成、国籍、郵便番号、職業、役職など | 低 | 低 | 低 | 出力時の加工は必要としない。 |
| 10 | 職歴・学歴 | 個人の職歴や学歴に関する情報 | 職歴、学歴 | 低 | 中 | 中 | マスク処理する。 |
| 11 | 位置情報 | GPS機器から計測される位置情報や携帯電話基地局の位置情報 | 位置情報(GPS)、携帯電話基地局情報 | 低 | 中 | 中 | マスク処理する。 |

図 4 アプリケーションログ出力指針

### 4.2 適用例

本指針の適用例を示す．実験に使用したサンプルアプリケーションは，Web ブラウザを使用し，書籍の注文を行う簡易な Web アプリケーションであり，Java 言語によって作成しており，ログの出力には log4j を使用している．ログの出力の内容は以下のとおりである．

年月日 時分秒 ログレベル ログカテゴリ名 処理名:
ログ出力項目 スレッド名(ソースファイル名:行番号)

ログの出力のタイミングは，ログイン，注文受付，ログアウトであり，処理名の箇所に出力される．指針適用前は，ログ出力項目に，ユーザーID，パスワード，書籍名，数量，送付先住所，備考をそのまま出力している．指針適用前のログ出力例を図 5 に示す．

2015-04-22 03:10:59,638 DEBUG com.mycompany.servlets.LoginServlet - ログイン: suzuki,suzuki [http-bio-8888-exec-8] (LoginServlet.java:63)
2015-04-22 03:11:53,355 DEBUG com.mycompany.servlets.ConfirmServlet - 注文受付: suzuki, プログラミング言語 Ruby, 1, 東京都港区赤坂１－２－３, 至急 [http-bio-8888-exec-10] (ConfirmServlet.java:76)
2015-04-22 03:11:55,486 DEBUG com.mycompany.servlets.LogoutServlet - ログアウト: suzuki [http-bio-8888-exec-5] (LogoutServlet.java:29)

図 5 指針適用前のログ出力例

指針適用後は，ユーザーID はハッシュ関数により符号化し，パスワードは出力せず，書籍名と送付先住所はマスク処理を施している．指針適用後のログ出力例を図 6 に示す．

2015-04-22 03:18:58,709 DEBUG com.mycompany.servlets.LoginServlet - ログイン:
d222a18d6474d0819d8ee5da0c2c524f31ff0903a4e6abc3f7957f84f1ee3f0f [http-bio-8888-exec-7] (LoginServlet.java:63)
2015-04-22 03:19:46,426 DEBUG com.mycompany.servlets.ConfirmServlet - 注文受付:
d222a18d6474d0819d8ee5da0c2c524f31ff0903a4e6abc3f7957f84f1ee3f0f, ＊＊＊, 1, 東京都＊＊＊＊＊＊＊＊＊＊, 至急 [http-bio-8888-exec-10] (ConfirmServlet.java:76)
2015-04-22 03:19:48,041 DEBUG com.mycompany.servlets.LogoutServlet - ログアウト:
d222a18d6474d0819d8ee5da0c2c524f31ff0903a4e6abc3f7957f84f1ee3f0f [http-bio-8888-exec-6] (LogoutServlet.java:29)

図 6 指針的適用後のログ出力例

マスク処理は，対象のデータを「＊」の文字に置き換え，伏せ字にしている．住所は上位 3 文字のみ表示し，書籍名は「＊＊＊」に変換している．また，ユーザーID を符号化するハッシュ関数には SHA256 を使用している．

## 5. 考察

前章で示したような加工を施すことによって，データの内容を秘匿しつつ，アプリケーションログからプログラムの実行状態を確認することができるメリットがある．ただし，システム開発・運用においては，設計・プログラミング・テストの作業工数の増加，データ加工処理に伴う実行時の性能の低下のデメリットも考えられ，それらの対策の検討も必要である．

さて，このようなプライバシーへ配慮した措置をおこなった場合，現在国会で審議されている個人情報保護法改正案[4]にて新たに導入された「匿名加工情報」との関係において問題が生じる可能性があるではないかと筆者は考える．以下，この点について解説する．

まず，「匿名加工情報」は改正案 2 条 9 項で以下のよう定義されている．

第 2 条
9 この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。
一 第 1 項第一号に該当する個人情報当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）
二 第 1 項第二号に該当する個人情報当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

図 7 匿名加工情報の定義

つまり，「匿名加工情報」とは，個人情報の一部を削除

したり他の記述に置き換えたりする加工をしたものであり，かつ当該個人情報を復元することができないようにしたものである．改正案 2 条 9 項は非常に広い範囲を示すと解釈でき，高木[16]は次のように述べている．「どんな状況であれ，どんな情報であれ，個人情報の一部を削除したり他の記述に置き換えたりする加工をすると，それが客観的に，元の個人情報を「復元することができないようにしたもの」と言えるものならば，いつでも「匿名加工情報」に該当する．加工方法はほとんど限定されておらず，一部を削除したり他の記述に置き換える加工は，何ら特殊なものではないので，ごく普通に誰でも日頃から「匿名加工情報」を何の気なしに作成していることになる．」

本稿で示したログ出力指針は，まさに個人情報の一部を削除したり他の記述に置き換えたりする加工であるため，出力内容しだいでは「匿名加工情報」に当たる可能性があるのではないかと考える．

また,「匿名加工情報」を作成または利用する事業者を「匿名加工情報取扱事業者」と呼び，改正案 2 条 10 項では以下のように定義している．

> 第 2 条
> 10 この法律において「匿名加工情報取扱事業者」とは、匿名加工情報を含む情報の集合物であって、特定の匿名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の匿名加工情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの（第 36 条第 1 項において「匿名加工情報データベース等」という。）を事業の用に供している者をいう。ただし、第 5 項各号に掲げる者を除く。

図 8 匿名加工情報取事業者

改正案 2 条 10 項によると，「匿名加工情報データベース等を事業の用に供している者」となっているため，本稿で示した方法でログを出力し，たまたま「匿名加工情報」となってしまった場合，個人情報取扱事業者は「匿名加工情報取扱事業者」となってしまう可能性があるのではないだろうか．

なお,「匿名加工情報取扱事業者」には，改正案 36 条-39 条の匿名加工情報取扱事業者等の義務が課せられる．36 条では匿名加工情報の作成について，37 条は匿名加工情報の提供について，38 条は識別行為の禁止，39 条は安全管理措置等の義務を定めている．36 条の匿名加工情報取扱事業者等における匿名加工情報の作成等に係る義務の内容は次のような内容である．

(1)匿名加工情報（匿名加工情報データベース等を構成するもの）を作成するときは，特定の個人を識別すること及びその作成に用いる個人情報を復元することができないようにするために，個人情報保護委員会規則で定める基準に従い，当該個人情報を加工する．
(2)匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに前項の規定により行った加工の方法に関する情報の漏えいを防止するために，個人情報保護委員会規則で定める基準に従い，加工の方法に関する情報の安全管理のための措置を講じる．
(3)匿名加工情報を作成したときは，個人情報保護委員会規則で定めるところにより，当該匿名加工情報に含まれる個人に関する情報の項目を公表する．
(4)匿名加工情報を作成して当該匿名加工情報を第三者に提供するときは，個人情報保護委員会規則で定めるところにより，あらかじめ，第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに，当該第三者に対して，当該提供に係る情報が匿名加工情報である旨を明示する．
(5)匿名加工情報を作成して自ら当該匿名加工情報を取り扱うに当たっては，当該匿名加工情報の作成に用いられた個人情報に係る本人を識別するために，当該匿名加工情報を他の情報と照合してはならない．
(6)匿名加工情報を作成したときは，当該匿名加工情報の安全管理のために必要かつ適切な措置，当該匿名加工情報の作成その他の取扱いに関する苦情の処理その他の当該匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ，かつ，当該措置の内容を公表するよう努める．

プライバシーに配慮して，個人情報の一部を削除したり加工して出力したログの内容が「匿名加工情報」に該当するとした場合，事業者の義務に関して以下の疑問がある．

・ログに出力する情報を個人情報保護委員会規則で定める基準で加工していない場合，法令違反となるのか．
・ログに含まれる個人に関する情報の項目を公表する必要があるのか．
・システム開発や運用は委託が想定されるが，システム障害の調査のためログを提供する場合も第三者提供となり，委託先に提供するログに含まれる個人に関する情報の項目及びその提供の方法について公表する必要があるのか．
・ログに出力しているユーザーID を障害の調査のために，マスタと照合してはならないのか．
・ログの取り扱いや安全管理措置の内容を公表する必要があるのか．

現時点(4 月 22 日現在)において，改正案は可決されていないため，条文の規定がより明確に修正されるか，個人情報保護委員会規則で具体化されることを期待する．情報漏えい対策およびプライバシーへの配慮としてログから個人の特定性を低減させる対策が，意に反して法的対応のコス

トを引き上げてしまっては本末転倒と言える．

## 6. まとめ

本稿では，アプリケーションログに出力する項目のプライバシーへの影響度を評価して，出力する情報を限定することにより，プライバシーリスクを低減することを目的とした，アプリケーションログ出力指針を提案した．ログから個人を特定する情報を削除および加工することにより，プライバシーリスクが低減されるため，情報漏えい対策としても有効と言える．システム開発・運用においては，設計・プログラミング・テストの作業工数の増加，データ加工処理に伴う実行時の性能の低下などへの対策も検討が必要である．

また，このように加工された情報が，個人情報保護法改正案における「匿名加工情報」にあたるのではないかという懸念から，「匿名加工情報」に該当する場合には，事業者が「匿名加工情報取扱事業者」の義務を負う必要があるのか，問題提起をした．本稿で指摘した問題が筆者の誤解，個人情報保護法の理解不足によるものであるならば，筆者の勉強不足をご容赦いただきたい．

## 参考文献

1) 経済産業省: 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン(2014 年 12 月)
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf
2) PCI Security Standards Council, LLC: Payment Card Industry（PCI）データセキュリティ基準(2013 年 11 月)
https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/PCI_DSS_v3.pdf
3) 日経コンピュータ: 今度は横浜銀行でカード偽造事件　問われる多重委託下の運用・管理体制，日経コンピュータ 2014 年 2 月 20 日号，日経 BP 社, pp.8(2014 年)
http://itpro.nikkeibp.co.jp/article/COLUMN/20140214/536782/
4) 内閣官房: 個人情報の保護に関する法律及び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の一部を改正する法律案新旧対照条文(2015 年 3 月)
http://www.cas.go.jp/jp/houan/150310/siryou4.pdf
5) ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements
6) JIS Q 27001:2014, 情報技術 - セキュリティ技術 - 情報セキュリティマネジメントシステム - 要求事項
7) ISO/IEC 27002:2013, Information technology - Security techniques - Code of practice for information security controls
8) JIS Q 27002:2014, 情報技術 - セキュリティ技術 ? 情報セキュリティ管理策の実践のための規範
9) 地方公共団体における情報システムセキュリティ要求仕様モデルプラン（Web アプリケーション），財団法人地方自治情報センター 自治体セキュリティ支援室(2012 年 10 月)
https://www.j-lis.go.jp/lasdec-archive/cms/resources/content/28369/webappsecmodel-1.0.pdf
10) アン・カブキアン: プライバシー・バイ・デザイ，日経 BP 社 (2012)
11) EU 一般データ保護規則提案,“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”, EU EUROPEAN COMMISSION(2012 年 1 月 25 日)
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
12) “Protecting Consumer privacy in an Era of Rapid Change”, 米国 FTC(2012 年 3 月)
http://ftc.gov/os/2012/03/120326privacyreport.pdf
13) 総務省：スマートフォン プライバシー イニシアティブ －利用者情報の適正な取扱いとリテラシー向上による新時代イノベーション－ (2012 年 8 月)
http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000087.html
14) 瀬戸洋一: 実践的プライバシーリスク評価技法―プライバシーバイデザインと個人情報影響評価―, 近代科学社, pp.30(2014)
15) NPO 日本ネットワークセキュリティ協会: 2013 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～, pp.50(2015 年 2 月)
http://www.jnsa.org/result/incident/data/2013incident_survey_ver1.2.pdf
16) 高木浩光: 匿名加工情報の規定ぶりが生煮えでマズい事態に（パーソナルデータ保護法制の行方 その 15），高木浩光＠自宅の日記(2015 年 3 月 10 日)
https://takagi-hiromitsu.jp/diary/20150310.html