SQAT®

情報セキュリティ瓦版

2018年7月号

株式会社ブロードバンドセキュリティ
セキュリティサービス本部
東京都新宿区西新宿 8-5-1 野村不動産西新宿共同ビル 4F
TEL：03-5338-7417 FAX：03-5338-7435
https://www.bbsec.co.jp/

PCI DSS バージョン 3.2.1 リリース
SSL/ 初期 TLS 廃止への対応、いよいよ待ったなしに

2018 年 5 月 17 日、PCI DSS のマイナーリビジョン ver.3.2.1 がリリースされました。

今回のリビジョンは、前バージョンの ver.3.2 において「2018 年 1 月 31 日まではベストプラクティスとするが、それ以降は要件とする」と注記されていた項目の期日が過ぎたこと、および SSL/ 初期 TLS の廃止期限（2018 年 6 月 30 日）を目前に控えたことによる、関連要件の更新が主な目的です（主な変更内容は表 1 をご参照ください）。

PCI DSS
（Payment Card Industry Data Security Standard）

2006 年、大手カード会社 5 社（American Express、Discover、JCB、MasterCard、VISA）が共同で設立した組織「PCI SSC」（Payment Card Industry Security Standards Council）によって策定、管理されているクレジットカード業界のデータセキュリティ標準。

SSL/ 初期 TLS の廃止

SSL/ 初期 TLS には、プロトコルの仕様自体やプロトコルがサポートする暗号化方式に既知の脆弱性が存在し、例えば、POODLE（Padding Oracle On Downgraded Legacy Encryption）攻撃や BEAST（Browser Exploit Against SSL/TLS）攻撃等を介して暗号化通信が解読される危険性があります。そのため、要件 2.2.3、2.3、4.1 で求められる「強力な暗号化技術」には該当しないとみなされ、既に PCI DSS ver.3.1 において、猶予期間を設けた上で廃止が求められていました。廃止について、ver.3.1 では当初、「2016 年 6 月 30 日まではベストプラクティス、同年 7 月 1 日以降は要件とする」と定めていましたが、20 年以上にわたり広く普及してきたプロトコルであることから対応には相応の時間が必要だと判断され、PCI DSS ver.3.2 において、「2018 年 6 月 30 日まではベストプラクティス、同年 7 月 1 日以降は要件とする」と猶予期間が 2 年延長されました。その期限が近づき、SSL/ 初期 TLS の廃止が要件へと変更されるため、今後の対応および例外について明文化した ver.3.2.1 のリリースが必要となったのです。

「初期 TLS」とは

PCI DSS では、「初期 TLS」のバージョンを具体的には明言しておらず、「既知のエクスプロイト（攻撃プログラム）に対して脆弱な TLS の実装あるいはバージョン」と定義しています。これは、日々進化する攻撃の脅威に対し、より強力な暗号化技術に対応したバージョンのプロトコルが開発され、普及することを想定しているためです。とはいえ、この定義だけではあまりにも曖昧であるため、「NIST Special Publication 800-52」等の情報セキュリティ基準で定められているプロトコルや設定を「強力な暗号化技術」の例として提示しており、現時点で推奨される TLS のバージョンは TLS 1.2 以上となっています。

「TLS 1.3」のリリース

2018 年 3 月、インターネット関連技術の標準化を進める任意団体 IETF（Internet Engineering

表 1：PCI DSS v3.2 からの変更内容

変更概要	変更概要	変更内容
3.6.2	誤記の修正	参照要件の誤記修正（3.5.1→3.5.2）
3.5.1、6.4.6、8.3.1、10.8、10.8.1、11.3.4.1、12.4.1、12.11、12.11.1	移行期間の削除	2018/02/01 までの ver.3.2 移行期間に関する記述の削除
2.2.3、2.3、4.1	猶予期間の削除	SSL/ 初期 TLS 廃止までの猶予期間に関する記述の削除 一部使用が認められる端末（POS POI 端末等）について追記
Appendix A2	猶予期間の削除	SSL/ 初期 TLS 廃止までの猶予期間に関する記述の削除 一部使用が認められる端末（POS POI 端末等）について追記
Appendix B	説明文の変更	MFA がすべての非コンソールアクセスに必要となったため、 " 代替コントロールとしての MFA" に関する記述を削除

Task Force）の承認を経て、TLS の新たなバージョン「TLS 1.3」が正式にリリースされました。

従来のバージョンではハンドシェイクプロトコルの全フェーズ完了後に暗号化通信が開始されていたのに対し、TLS 1.3 では最初の鍵共有フェーズ完了以降、データのやり取りがすべて暗号化されます。これにより、攻撃者はパラメータフェーズ、認証フェーズのデータを盗聴できなくなるため、達成される安全性のレベル向上が見込まれています（『SQAT® 情報セキュリティ瓦版 2018 年 5 月号』を参照）。

TLS 1.3 は、「より強力な暗号化技術」として、現在 Google Chrome や Firefox 等の Web ブラウザ側、および多くの企業・サービス等で対応が進んでいます。今後 TLS 1.3 の普及が進み、さらに TLS 1.3 よりも強力な全く新しいプロトコルが開発された場合、現在推奨されている TLS 1.2 も危殆化して「初期 TLS」の部類に入るときが来るかもしれません。PCI DSS において「強力な暗号化技術」の使用が要件とされる目的は、伝送、処理、または保管されるカード情報の保護です。準拠に取り組む組織は、常にこのことを念頭に置き、情報収集や対策の実施を行うことが重要です。

PCI DSS 準拠

準拠にあたっては、認定評価機関 QSAC（Qualified Security Assessors Company）による審査と、認定スキャニングベンダー ASV（Approved Scanning Vendor）による外部ネットワーク脆弱性スキャンに合格しなければなりません。

PCI DSS ver.3.2.1 では、ASV スキャンで SSL/ 初期 TLS が検出された場合、基本的には「不合格」と判断されます。ただし、何らかの制約によって SSL/ 初期 TLS を廃止できない場合、運用する環境や代替策により、例外として継続利用が認められ「合格」の評価を得られることがあります。

【例外として認められる例】

- SSL/ 初期 TLS が、PCI DSS 要件のセキュリティ対策を満たす以外の目的に使用されている場合
- SSL/ 初期 TLS が POS POI 端末およびサービスプロバイダの接続ポイントで使用されており、かつ既知の脆弱性に対して影響を受けない場合
- SSL/ 初期 TLS での通信を行う前に、強力な暗号化技術を使用してデータを暗号化している場合（例：フィールドレベルやアプリケーションレベルでの暗号化）
- 先に強力な暗号化が施されたセッションを確立し（例：IPSec トンネルの構築）、そのセッション内において SSL/ 初期 TLS でデータ通信を行う場合

なお、上記のようなケースに該当しても、「使用するバージョンの SSL/ 初期 TLS に存在する既知の脆弱性に対してセキュリティパッチを適用する」等の対策は変わらず実施する必要があります。例えば、CVSS 基本値 4.0 以上の脆弱性、または「高」リスクに分類される脆弱性が解消されていない場合、ASV スキャンで合格することはできません。また、QSAC あるいは ASV によって「代替コントロールが不十分」と判断された場合にも合格とはなりません。

今回のリリースに伴い、組織として特に早急に対応を進めるべきと考えられるのが、「2018 年 6 月 30 日以前に準拠を済ませており、PCI DSS 要件を満たすためのセキュリティ対策として SSL/ 初期 TLS を使用している」場合です（次年度に審査を受ける場合、PCI DSS のバージョンは 3.2.1 となる）。次回審査まで時間があったとしても、SSL/ 初期 TLS 廃止のデッドラインは過ぎているため、対策を行わない限り ASV スキャンでは不合格となり、結果、準拠を名乗ることはできなくなります（準拠には、四半期に一度の ASV スキャンの全てで「合格」の評価を得ることが必要）。

PCI DSS の今後の展望

PSI SSC の最高技術責任者（CTO）トロイ・リーチ氏は、「セキュリティを強化することでカード会員データに対する攻撃の“魅力を低減”し、攻撃者が当該情報を容易な標的と考えなくなるような解決策を見出していくこと」を目標に、PCI セキュリティ基準を発展させていくと述べています。同氏によれば、次回メジャーリリースの予定は 2020 年以降になるそうですが、それまでにも、今回の ver 3.2.1 のようなマイナーリビジョンがリリースされる可能性がないとはいえません。改訂の状況、リリース時期などについて定期的に情報を収集していくことが求められるでしょう。

参考情報：

https://blog.pcisecuritystandards.org/pci-dss-now-and-looking-ahead

https://www.pcisecuritystandards.org/pdfs/15_12_18_SSL_Webinar_Press_Release_FINAL_%28002%29.pdf

https://tools.ietf.org/html/draft-moriarty-tls-oldversions-diediedie-00

****

BBSec は QSAC として 10 年以上の実績を持ち、PCI DSS 準拠支援、脆弱性診断など、組織の情報セキュリティ向上を支援するサービスをワンストップで提供しています。セキュリティに関わる課題がございましたらお気軽にご相談ください。

GDPR に続き審議が進む「e プライバシー規則」とは？

2018 年 5 月 25 日、欧州連合（EU）により一般データ保護規則（GDPR）* が施行されました。

GDPR は、企業に対して欧州経済領域（EEA）域内の個人データの保護に関する規則の遵守を義務付けるもので、同経済領域内でのサービス提供の有無を問わず、全世界の企業が対象になりえます。

違反した場合は巨額の制裁金が科されるのが大きな特徴で、制裁を回避するために EU からのアクセスを遮断する Web サイトが出るなど、施行以降世界各地で準拠をめぐる混乱が生じており、同規則が軌道に乗るまでには暫く時間がかかるものと見込まれます。

そうした中、同様に個人情報の保護を目的とする、新たな規則の施行が近づいています。GDPR の特別法として位置づけられる「e プライバシー規則（ePrivacy Regulation）」（通称：「Cookie 法」）です。同規則は、電子通信に関わる領域におけるプライバシーの保護を目的とするものです。

GDPR と同じく、e プライバシー規則は EU の法令の一部です。EEA 域内の個人の情報を保護する法律ではありますが、グローバルに情報がやり取りされる現代においては、あらゆる経済圏に影響が及びます。さらに、同規則の対象となる電子通信サービスが、近年さらなる広がりを見せていることにも留意する必要があります。

Web サービスのみならず、OTT（Over The Top）サービス、メッセージングサービス、Web メール、ネット配信による動画サービス等でも遵守が求められることになるのです。規則の主旨やスコープを理解して、着実に準備を整えていく必要があるでしょう。

*** 一般データ保護規則（GDPR：General Data Protection Regulation）**

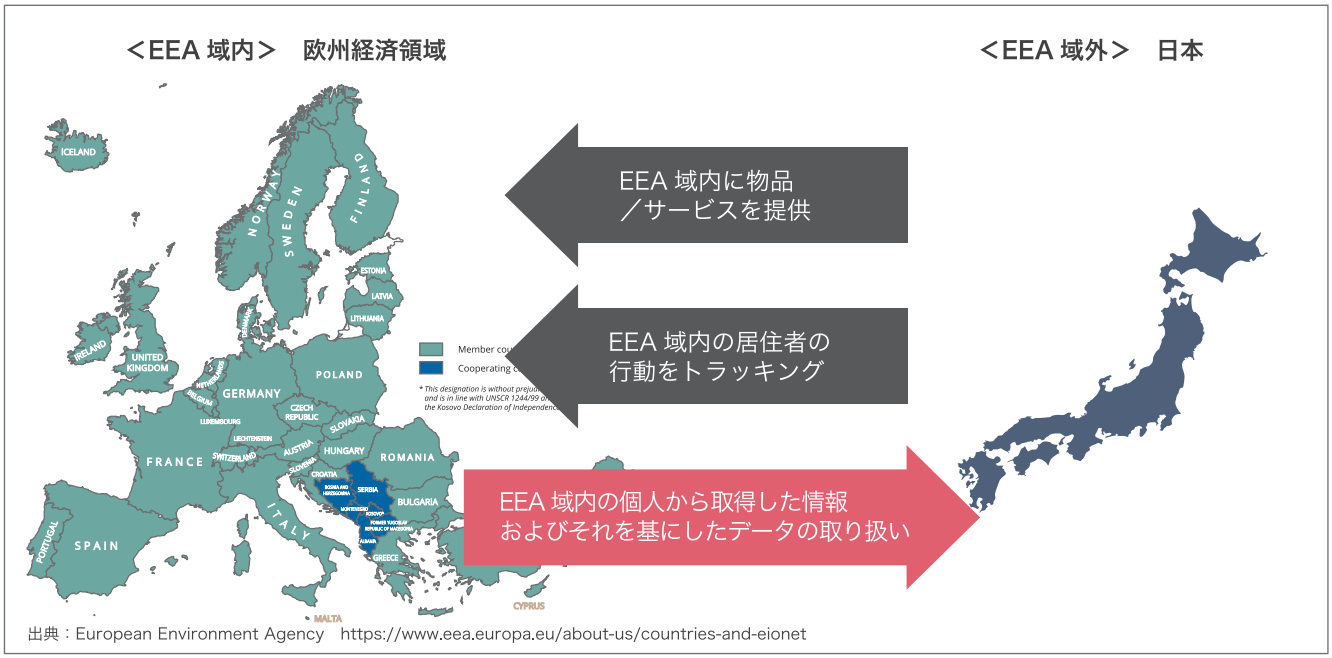
欧州連合（EU）の条約において、一般的な企業活動に伴う個人の情報を保護するための規則

e プライバシー規則とは一体どういうものなのでしょう。そして、なぜ「Cookie 法」と呼ばれているのでしょう。

e プライバシー規則の背景

e プライバシー規則の発端は、2015 年に EU が発表した「デジタル単一市場（DSM）戦略」にさかのぼります。同戦略は、EU 加盟国間のデジタル市場を統合し、人、モノ、資本、サービスの自由な移動を実現させ、EU デジタル経済の発展を目指すものです。その促進のためには電子識別・認証の相互認証、電子署名指令に関する見直しが欠かせないとの認識の

GDPR の施行は日本の企業活動にも影響する



出典：European Environment Agency　https://www.eea.europa.eu/about-us/countries-and-eionet

もと、個人データ保護とプライバシーに関する法令の整備が進められてきました。

そうした流れを経て、2018 年 5 月に施行された GDPR に続き、成立に向けた取り組みが進められているのが「e プライバシー規則」です。現時点では「指令」（「e プライバシー指令」）のもと適用されていますが、今後「規則」に格上げされることにより、遵守の手続きや違反した場合の制裁などが明確に規定されることになります。

前述したように、e プライバシー規則は「電子通信」における規則であるため、ビジネスにインターネットを使用している全ての企業が対象になりえます。これはある意味、「ビッグデータ」の時代に逆行する規制ともいえ、「商業活動を阻害する」として、EU 域外の国々のみならず EU 域内の企業からも懸念が表明されています。そうした懸念を受け、現在は修正を繰り返しながら、成立に向け審議が進められている状況です。

EU が、GDPR をはじめとする各種法令で保護対象と定めている情報は右表のとおりです。赤字（GDPR では保護対象となっているが、日本の個人情報保護法では保護対象ではないもの）にご注目ください。多額の制裁金が科される法規制の施行にあたり、企業は保護される個人情報の定義について、改めて認識しておく必要があるでしょう。

e プライバシー規則に至る流れ

1993 年 1 月	「単一市場」の発足
2002 年 7 月	e プライバシー指令（2002/58/EC）制定
2011 年 4 月	「デジタル単一市場（DSM）戦略」の主要分野を発表
2016 年 5 月	一般データ保護規制（GDPR）の採択
2017 年 1 月	e プライバシー規則案を発表
2017 年 10 月	欧州議会、修正した e プライバシー規則案を承認
2018 年 3 月	修正後の e プライバシー規則案を発表
2018 年 5 月	一般データ保護規制（GDPR）の施行

GDPR（EU）／個人情報保護法（日本）対象データ対比一覧

○: 保護対象／△: 他の要素との組み合わせにより保護の対象となる／×：保護対象外
赤字：GDPR では保護対象となっているが、個人情報保護法では保護対象ではないもの

情報の種類（日本の事業者が取り扱う個人情報）	個人情報保護法（日本の事業者が取り扱う個人情報）	GDPR（EEA 域内の個人情報）
氏名	○	○
住所	△	○
電話番号	△	○
携帯電話番号	×	○
生年月日	○	×
銀行の口座番号	×	○
クレジットカード番号	×	○
運転免許証番号	○	○
保険証番号	○	○
パスポート番号	○	○
社会保障番号	○	○
年金番号	○	○
マイナンバー	○	ー
住民票コード	○	ー
顔写真	○	×
メールアドレス	△	○
IP アドレス	×	○
Cookie	×	○
GPS によるトラッキングデータ	×	○
DNA	○	○
虹彩	○	○
声紋	○	○
指紋・掌紋	○	○
手指の静脈	○	○
歩行形態	○	○
人種	○	○
民族	○	○
社会的身分	○	○
病歴	○	○
犯罪歴	○	○
宗教・社会的信条	○	○
身体的・知的・精神的障害に関する情報	○	○
医療情報	○	○
刑事事件･少年事件の関係者としての履歴	○	○
性的嗜好	○	○
収入に関する情報	○	○
労働組合員資格	×	○
代理人を必要とする子供の年齢	12 歳～ 15 歳（ガイドラインによる）	13 歳～ 16 歳

e プライバシー規則の構成

続いて、e プライバシー規則の内容を具体的に見ていきましょう。

まず適用対象ですが、これは第 2 条に明記されています（「適用対象」参照）。大きく見ると、電子通信サービスで扱われる個人に関する情報、および、その情報を扱う行為が、幅広く対象になっているといえるでしょう。その中で、先に述べた懸念の的になっているのが 1）の項目です。理由は、企業の営業やマーケティングに欠かせない「Cookie」がターゲットになるためです。Cookie には、Web サービスの利用者の情報が保持され、それらのデータはより効果的な事業活動のために利用されます。ここに大きな規制がかかることは企業にとって大打撃であり、そのインパクトは多大です。同規則が「Cookie 法」の通称で広まっているのには、このような事情があります。

さらに知っておきたいのが、同規則における「電子通信データ」の定義です。リスト（「主な定義」参照）に示したように「コンテンツ」と、コンテンツをやり取りする目的で処理される「メタデータ」の 2 つが挙げられています。Cookie は、まさにこのメタデータに当たります。

e プライバシー規則が施行された場合、一部の例外（ログイン情報を保存する場合など）を除き、ユーザの同意は必須となり、違反した場合には巨額の制裁金が課されます。また、Cookie の利用についてユーザの同意を得られなかったとしても、同意を得た場合と同様にサービスを提供し続ける必要があります。つまり、サービス提供時に Cookie を使って直接的 / 間接的にメリットを得ることを、従来のようには期待できなくなるわけです。

来たるべき施行に向けて

今後施行されるであろう e プライバシー規則への対応では、企業はサービスの仕様や設計の見直しを迫られることになるでしょう。影響範囲は広く、相応のコスト・時間がかかる可能性があり、技術や運用に関してさまざまな意思決定を行う必要が出てくると見込まれます。そうした意思決定にあたっては、同規則の主旨を理解しておくことが助けになるでしょう。

繰り返しになりますが、同規則の大きな目的は、「エンドユーザのプライバシーを保護する」ことです。その目的のもと、当事者以外がデータを処理することが原則として禁じられ、何らかの処理をする場合には当事者の同意を得ることが求められます。これが、「同意が必須」の背景です。

したがって、同意の確認が求められるのは、エンドユーザの端末に含まれる情報だけではありません。企業システムの側に情報を保持する際も同意が必要になります。一時的な処理のために情報を使用した場合にそれを消去する必要もあります。こうしたことが複数の条項として明文化されているわけですが、条項ごとに個別的対応を検討するよりも、上記の大目的に鑑みて、自社事業におけるエンドユーザの情報の運用を包括的な観点から見直すことが効果的な対応につながるといえるでしょう。

また、「プライバシーの保護」が課題として取り組まれてきた背景を理解しておくことも有用です。まず前提にあるのは、すべての人にはプライバシー、すなわち、私的な生活をみだりに公開されない権利がある、という考え方です。プライバシーの侵害は、誹謗中傷、脅迫被害など、さまざまな問題を引き起こしますが、インターネット社会においては、しかるべき規制がなければ、人々はそうした脅威に世界規模で、かつ、物理的制約なくさらされ続けることになります。こうした問題を解決、軽減していくためには、インターネットを利用するエンドユーザが、「自分に関する情報を知られてよいか知られたくないかを、自らコントロールする権利」を保証する必要があるのです。

したがって、事業でインターネットを利用する企業に今後求められるのは、エンドユーザのプライバシーが守られることを保証する、信頼度の高いサービスです。安定した事業継続のためには、IT システムで電子通信におけるプライバシー保護を実現すると同時に、経営課題としてプライバシー保護に対する認識を徹底させていかなければなりません。

データが企業の命運を分ける時代、ビッグデータによるビジネスチャンスの拡大に目を向けるだけでなく、同等に重要な課題として、個々のエンドユーザのプライバシー保護に取り組むことも必須といえます。

参考情報：

https://www.parlament.gv.at/PAKT/EU/XXV/EU/12/90/EU_129000/imfname_10686084.pdf

https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/00/EU_30006/imfname_10827644.pdf

https://www.parlament.gv.at/PAKT/EU/XXVI/EU/01/58/EU_15804/imfname_10796438.pdf

http://www.nihonjinkai.be/file/jetro/seminar2017_1_shiryo1.pdf

適用対象（第２条より）

1）電子通信サービスの提供・使用に関連して送信される電子通信コンテンツの処理、および、同サービスの提供・使用に関連して実行されるメタデータの処理
2）エンドユーザが所有する端末機器で処理、送信、保存される情報
3）電子通信を許可するソフトウェアの販売（インターネット上の情報の検索、表示等）
4）電子通信サービスのエンドユーザに関する公開ディレクトリの提供
5）ダイレクトマーケティングに関わる情報の送信、表示

■主な定義（第４条より）

「電子通信データ」とは、「電子通信コンテンツ」と「電子通信メタデータ」を意味する

1）電子通信コンテンツ
電子通信サービスによってやり取りされるテキスト、音声動画、画像、音声など

2）電子通信メタデータ
電子通信サービスによって、電子通信コンテンツを送信、配布、やり取りする目的で処理される以下のようなデータ
・通信元や通信先を追跡・特定するために使用されるデータ
・電子通信サービスの提供時に生成される通信機器の場所に関するデータ
・通信の日時、期間、通信種別

e プライバシー規則の各条項に違反した場合の課徴金（第 23 条より）

・電子通信データの処理に係る違反（第８条） ・ソフトウェアプロバイダーの義務違反（第 10 条） ・公開ディレクトリに関する違反（第 15 条） ・電子通信サービスの利用に係る違反（第 16 条）	1,000 万ユーロ、または前会計年度 全世界年間売上高の 2%、いずれか高い方
・通信の秘密の侵害（第５条） ・通信の秘密の例外の濫用（第６条） ・電子通信データにおいて必要な消去を行わなかった場合（第７条）	2,000 万ユーロ、または前会計年度 全世界年間売上高の 4%、いずれか高い方

SQAT®（Software Quality Analysis Team）とは
～スペシャリスト集団が組織の脆弱性対策をトータルに支援～

「SQAT®」は、BBSec がご提供する脆弱性診断サービスです。エンジニア、コンサルタント、ホワイトハッカー等から編成された精鋭チームが、あらゆる側面から網羅的な診断を実施。スペシャリストのノウハウを結集して組織の情報システム強化をお手伝いします。お客様は金融機関・インターネット事業者などの民間企業から、官公庁をはじめとする公共機関まで幅広く、これまでに延べ 3,500 組織、1 万2千を超えるシステムで利用されています。

※ 本誌において記載されている会社名、商品名、サービス名は各社の商標又は登録商標です。なお、本文中では商標又は登録商標を表すマークを特に提示していない場合があります。

この冊子は、クリエイティブ・コモンズ表示 4.0 ライセンスの下に提供しております。
二次利用にあたっては、出典明示（出典：株式会社ブロードバンドセキュリティ発行『SQAT® 情報セキュリティ瓦版』）をお願いします。
また、商用利用は許諾しておりません。

SQAT® は BBSec の登録商標です。登録商標第 5146108 号

株式会社ブロードバンドセキュリティ　お問合せ電話番号　03-5338-7417