サイバーセキュリティと個人情報保護

畠中伸敏［著］

日科技連

まえがき

個人情報保護法を起案した堀部政男は，日本の保護法と EU の「一般データ保護規則（General Data Protection Regulation : GDPR）」の違いについて，「日本の個人情報保護法の成立は，早稲田大学で開催された江沢民の“宴の宵”への参加者名が流出したことが経緯となっており，EU の場合は，ユダヤ人大量虐殺のホロコーストが経緯となっている.」と述べたが，GDPR は日本の個人情報保護法に比べて，罰則などが厳しめである.

加えるに，法律の“建て”が違っている．日本の法律では，個人情報の漏洩は委託元に責任があるというのに対して，EU は個人情報の取扱者を管理者と処理者の 2 つに分け，この両方に対して，主務所のアクションを直接取れるようにしている．本書は，このことを念頭において，お読み願いたい.

さらに，最近のサイバー攻撃は，個人情報の漏洩と結びつくことが多く，この観点でも，いかに，情報セキュリティ技術を用いて，サイバー攻撃対策を行うかについても，その方法を紹介した.

ところで，平成 29（2017）年 5 月 20 日の「個人情報保護法」の改正に伴って，同年 12 月 20 日に「個人情報保護マネジメントシステム―要求事項」が改正された.

情報セキュリティマネジメントシステム（ISMS）の保護の対象は企業活動の基となる「情報」であり，個人情報保護マネジメントシステム（PMS）は本人が所有し本人の自己の管理下に置かれるべき「個人情報」である．PMS ではリスクを「個人情報リスク」と定義し，ISMS では「リスク」の定義を ISO 31000 の定義に準拠しマネジメントシステムの欠陥により生じる統制リスクの考え方を導入している.

しかし，平成 29 年 12 月 20 日に改正された「個人情報保護マネジメントシステム―要求事項」は ISMS との差異や矛盾点を解消することなく，受審側の運用や審査現場での課題を残すこととなった.

一方，EU では，1998 年に実施した EU データ保護指令を 2018 年 5 月 24 日に廃止した．これに代わり，2016 年 5 月 24 日に発効した，欧州経済領域（European Economic Area: EEA，EU 加盟国 28 カ国，ノルウェー，アイスランド，リヒテンシュタイン）から個人データを域外に持ち出すことを原則禁止する GDPR を，2018 年 5 月 25 日に施行した．

日本が「十分性認定」を受けることで，EEA 圏在住者の同意をもとに個人データの利用が可能となる．しかし，日本企業の 80% が対策を終えていないことから，GDPR に違反すると，最大で全世界の年間売上高の 4% もしくは 2,000 万ユーロ（高額なほうを適用）の制裁金が課せられる．このように，違反に伴う制裁金や訴訟などの新たなリスクの懸念を生じている．

この状況下で，日本の改正個人情報保護法，JIS Q 15001：2017 では，日本企業が EU 域内から，EU 域外へ個人データを移転する場合は，利用目的や取得の経緯を記録する．日本では，匿名のデータに加工する場合は，元の個人情報と加工済みデータの関係を復元できない，とされた．

一方，GDPR では，「プライバシー・バイ・ザイン」，「オプトイン原則」，「個人情報漏えい時の通知義務」，「データ持ち運びの権利」，「忘れられる権利」，「罰則の強化」への対応を求めており，未対応な企業にとって日欧間のデータ移転のさらなる障壁となる．

本書では，JIS Q 15001：2023 対応を配慮し，「パブリッククラウドにおける個人識別情報保護の実践規範」（ISO/IEC 27018），「個人識別可能な情報保護の実践規範」（ISO/IEC 29151），「プライバシー影響評価」（PIA，ISO/IEC 29134），「プライバシー保護の枠組み及び原則」（ISO/IEC 29100：2011（JIS X 9250））を解説し，個人情報のフレームワーク，用語の整合性を図る．

次に GDPR の対応策を示唆し，個人情報保護の新たなるリスクの懸念を払拭する．

本書の第 7 章の標的型攻撃メール訓練の URL 型メールの文案例については松田利夫氏（元 山梨学院大学教授）から，付録 1 については永井庸次氏（元 日

立製作所ひたちなか総合病院院長）から資料提供を受けた．感謝の意を表します．

末筆となるが，本書の出版および編集にあたって，多大なる協力をいただいた，日科技連出版社社長の戸羽節文氏，出版部長の鈴木兄宏氏，課長の石田新氏に，厚くお礼申し上げます．

2025 年 11 月吉日

湯河原にて

畠 中 伸 敏

サイバーセキュリティと個人情報保護
目　　次

まえがき……iii

第１章　サイバーセキュリティとは …… *1*

1.1　サイバーセキュリティとは　*2*
1.2　悪意のあるスキャンの増大　*3*
1.3　サイバー攻撃を受けた場合の被害　*4*
1.4　今後の対策　4
参考文献　*5*

第２章　個人情報の仮名化と匿名性 …… *7*

2.1　データ主体(=PII 主体)　*8*
2.2　仮名化　*10*
2.3　匿名加工情報　*12*
2.4　国内での匿名加工情報の法制化　*13*
2.5　匿名化のリスク　*17*
2.6　秘密計算　*20*
参考文献　*21*

第３章　GDPR の法的リスク ……23

3.1　EU のデータ保護の流れ　*24*
3.2　EU データ保護指令から一般データ保護規則(GDPR)への変更点　*26*
3.3　個人データ処理の原則，データ主体の権利　*26*
3.4　巨額の制裁金条項　*31*
3.5　制裁金の適用ルール　*40*
3.6　DPO(個人データ保護責任者)　*45*
3.7　広範な域外適用ルール　*49*

3.8　欧州委員会が認めた十分性認定　52
3.9　補完的ルール　54
3.10　Pマーク審査のポイントと対応　63
参考文献　65

第４章　脆弱性診断サービスおよびペネトレーション……67
4.1　脆弱性の重要性のランク　68
4.2　共通脆弱性タイプ一覧(CWE TOP 25)　74
4.3　脆弱性診断ツール　74
4.4　共通脆弱性評価システム(CVSS)　79
4.5　ペネトレーションとは　80
4.6　陥りやすい設定　84
参考文献　84

第５章　データ保護影響評価……87
5.1　GDPR の DPIA(データ保護影響評価)と規格の PIA(プライバシー影響評価)の違い　88
5.2　GDPR の DPIA の必要性　89
5.3　PIA(プライバシー影響評価)とは　93
5.4　PIA のプロセス　94
参考文献　113

第６章　ランサムウェアとその対策……115
6.1　ランサムウェアとは　116
6.2　ランサムウェアの攻撃事例　116
6.3　ねらわれた病院のシステム上の脆弱性と障害プロセス上の欠陥　126
6.4　ランサムウェアへの対策　129
参考文献　130

第７章　不正メールの形態と標的型攻撃訓練メールの文章パターン …… *131*

7.1　不正メールの特徴　*132*

7.2　不正メールへの対策　*132*

7.3　標的型攻撃訓練メール（URL 型）の文案作成例　*135*

第８章　標的型攻撃の訓練 …… *145*

8.1　標的型攻撃訓練メールのタイプ　*146*

8.2　標的型訓練の手順　*146*

8.3　不正メールの特徴（例）　*148*

8.4　警告文（教育用文書）（例）　*150*

8.5　報告書の内容　*153*

8.6　訓練による効果　*153*

参考文献　*154*

付　　録 …… *155*

付録１　令和７年度版医療機関におけるサイバーセキュリティ対策チェックリスト　*156*

付録２　平成二十六年法律第百四号　サイバーセキュリティ基本法　*159*

索　　引 …… *177*

4.1　脆弱性の重要性のランク

取り扱う脆弱性とは，開発された Web やアプリケーションに起因する Web やアプリケーション上の脆弱性で，ハッカーやサイバー攻撃がつけ入る要因となるものである．これには，プログラムのバグ，システム設定上のコンフギュレーション，変数の設定，想定した使用者への配慮事項の欠如など多岐にわたる．

OWASP（The Open Web Application Security Project：国際ウェブセキュリティ標準機構）は，世界中に数百の支部をもち，数万名の会員で構成されている非営利団体である．その目的は，アプリケーションや API を開発，購入，維持できるよう支援することである．OWASP は，Web やアプリケーションの脆弱性の致命度の上位 10 項目を OWASP TOP 10 として 2017 年と 2021 年に発表した[5]（**図表 4.1**）．なお，2025 年秋に TOP 10 が更新された．

また，1999 年頃から米国政府の支援を受けた非営利団体の MITRE は，40 以上のベンダーや研究機関の協力のもとに，2021 年，脆弱性を一覧表にした共通脆弱性タイプ一覧（CWE：Common Weakness Enumeration）を発表した．脆弱性の上位 25 項目を CWE TOP 25 と称する[7]．

OWASP TOP 10 の 2017 年度と 2021 年度を比較すると，2017 年度の第 1 位はインジェクション（Injection）であったが，2021 年度には第 3 位となり，アクセス制御の不備が第 1 位となっている．2017 年度に A3：2017- 機微な情報の露出が第 3 位であったが，2021 年度では，第 2 位の A02：2021- 暗号化の失敗という名称に変化した．

同様に，OWASP TOP 10 の 2021 年度と 2025 年度を比較すると，2021 年度の第 1 位はアクセス制御の不備で，2025 年度もアクセス制御の不備が第 1 位となっている（**図表 4.2**）．4 年間の順位が減少しないことから，この脆弱性の対策に苦慮していると思われ，全体的には，2021 年度に，A06：2021- 脆弱で古くなったコンポーネントと A10：2021- サーバーサイドリクエストフォージェリ（SSRF）が TOP10 入りしていたが，2025 年度は順位を下げ，2025 年度

では，時代を反映して，A03：2025- ソフトウェアサプライチェーンの失敗が，OWASP TOP 10 の第 3 位に順位を上げている．

それぞれの年度で，全世界に発生した脆弱性を収集して，致命度と重要性のランクを定めている．

OWASP TOP 10 および CWE TOP 25 は，ソフトウェアアーキテクト，デザイナー，開発者，テスター，ユーザー，プロジェクトマネージャー，セキュリティ研究者，教育者，および標準開発組織(SDO)にとって，ハッカーやサイバー攻撃のリスクの軽減に役立つ有用な示唆を与えている．

A01：2021- アクセス制御の不備[5],[8]は，2017 年度第 5 位(アプリケーションのセキュリティ)から 2021 年度は第 1 位となった．94% のアプリケーションがテストされ，テストされたアプリケーションの 3.81% の 1 つ以上の共通脆弱性タイプ一覧(CWE)をもち，このリスクカテゴリに該当する CWE は，テストされたアプリケーション 318,000 件以上で存在した．

- CWE-200：権限のない攻撃者への機密情報の漏洩
- CWE-201：送信データへの機微な情報の挿入
- CWE-352：クロスサイトリクエストフォージェリ

A02：2021- 暗号化の失敗は，2021 年度は第 2 位(アプリケーションのセキュリティ)である．暗号化（またはその欠如）に関連する障害であり，多くの場合，機密データの漏洩やシステム侵害につながる．

- CWE-259：ハードコードされたパスワードの使用
- CWE-327：壊れた，または危険な 暗号アルゴリズム
- CWE-331：不十分なエントロピー [5],[8]

A03：2021- インジェクションは，2021 年度の順位は第 3 位(アプリケーションのセキュリティ)に下がっている．テストされたアプリケーションの 94% で何らかのインジェクションに関する問題が確認されている．テストされたアプリケーションの最大発生率は 19%，平均発生率は 3.37% であり，このカテゴリに当たる 33 の CWE は，アプリケーションでの発生数が 2 番目に多く見られる．発生数は 27 万 4 千件であった．2021 年度では，クロスサイト

8.1　標的型攻撃訓練メールのタイプ

訓練対象者に訓練メールを踏ませる方法により，大まかに，次の 3 つに分類される．

(1)　URL 型

訓練対象者の関心事や業務を深く考察し，現実性と心理的な誘導を最大限に高め，URL のクリックを誘導する訓練メール．URL をクリックすると，発信元のサーバとリンクし，URL のパラメータやペイロード(画面に入力する値)により，識別子を忍ばせ，訓練対象者を同定する．**第 7 章**に例を示している．

(2)　添付ファイル型

訓練対象者の関心事や業務を深く考察し，現実性と心理的な誘導を最大限に高め，添付ファイルの開封を誘導する訓練メール．主に，添付ファイルにトラッキングなどのスクリプトを忍ばせ，添付ファイルを開封すると，発信元のサーバが開封の有無を検知する．**8.2 節**以降に示す．

(3)　混合型

上記の(1)および(2)を含めた訓練メール．

8.2　標的型訓練の手順

ツールとしては，ハッカー用 OS といわれる kali linux 上で動作する Gophish が代表的であるが，ここでは，広告で使われるトラッキングの手法を紹介する．トラッキングは，自社の広告が，一般消費者に閲覧されたかを確認するためなどに使用される．

マイクロソフトの Word や Excel は，面倒見がよい分，攻撃者はいろいろな側面から攻撃でき，逆に Mac OS の場合は OS 自体の機能が制限されるため，攻撃方法が制限され，その分，安全性が高いともいえる．従来型の攻撃で

はマクロや exe ファイルを送りつけていたが，最近は，マイクロソフトが対応策をとり，マクロがマイクロソフトの Office で検出されるようになった．

標的型訓練の手順例（トラッキングによる方法）

①　訓練対象者に送付する訓練用メールの本文および添付ファイルを開いた場合の Word の警告文（あるいは教育用文書）を作成する．

②　以下の Web ビーコンを Word に埋め込む[1]．

```
<html>
<head><title></title></head>
<body>
<img src=“画像の URL” width=” 1” height=” 1”>
<（自己のサーバ上の画像）>
</body>
</html>
```

例えば，自己のサーバに画像を保存し，幅 1，高さ 1 の画像として html から呼び出し，スクリプトを html ファイルに記載する．作成した html ファイルを Word で開くと，html で記載したものは実行され，幅 1，高さ 1 の点画像として実行される．このファイルを Word ファイルとして保存すると，Word のファイルとなり，Word への埋め込みが完成する．

③　Word の添付ファイルを訓練対象者に送付する．

④　Word のファイルの開封時に「警告文」の保護レビューが表示されるが，警告を無視して，訓練対象者がファイルを開封すると，添付ファイルに識別子が埋め込まれていて，訓練対象者の識別子が C&C サーバ上にログとして蓄えられる．このログ上に訓練対象者が踏んだことが検出される．なお，訓練対象者が Windows の Word などを用いている場合，保護ビュー（編集可能状態にする）をクリックすると，安全な場所（サンドボックス）の中にあったドキュメントが外に出され，トラッキングに埋め込まれた識別子が C&C にログとして記録される．しかし，訓練対象者が保護ビューをクリックしない

場合は，ドキュメントの文書を“開いて”も（ドキュメントを参照するのみでは），トラッキングに埋め込まれた識別子が C&C にログとして記録されない．Windows の保護ビューを避けたい場合は，保護ビューがない html などを添付ファイルとして使用する方法もある．

⑤　訓練の対象者に警告文が表示される．

8.3　不正メールの特徴（例）（図表 8.1 参照）

メールの本文は疑似メールであることから，不正メールの特徴を注意深く見ると，疑似メールであることがわかる．

①　@（アットマーク）以下のドメイン名が正規のものでない．

例えば，株式会社日科出版の正規のドメイン名は「juse-pub.jp」であるが，「juce-pub.jp」となっている．

②　内容が不自然（見覚えのないメール内容）

給与明細は通常，サイトが設けられていて，明細書が送られることはない．

③　ログインあるいは URL のクリックを誘導する．

メール本文が給与明細書のクリックを急がせる．

図表 8.1 に，標的型メール攻撃の例を示す．**7.2 節文案 4**（p.138）と併せて参考にしてほしい．

第 1 のポイント：メールの差出人に注意

偽装メールはドッペルゲンガー（なりすまし）ドメインを使用している．

正しいドメイン：@juse-pub.jp

なりすましのドメイン：@juce-pub.jp

第 2 のポイント：件名に注意

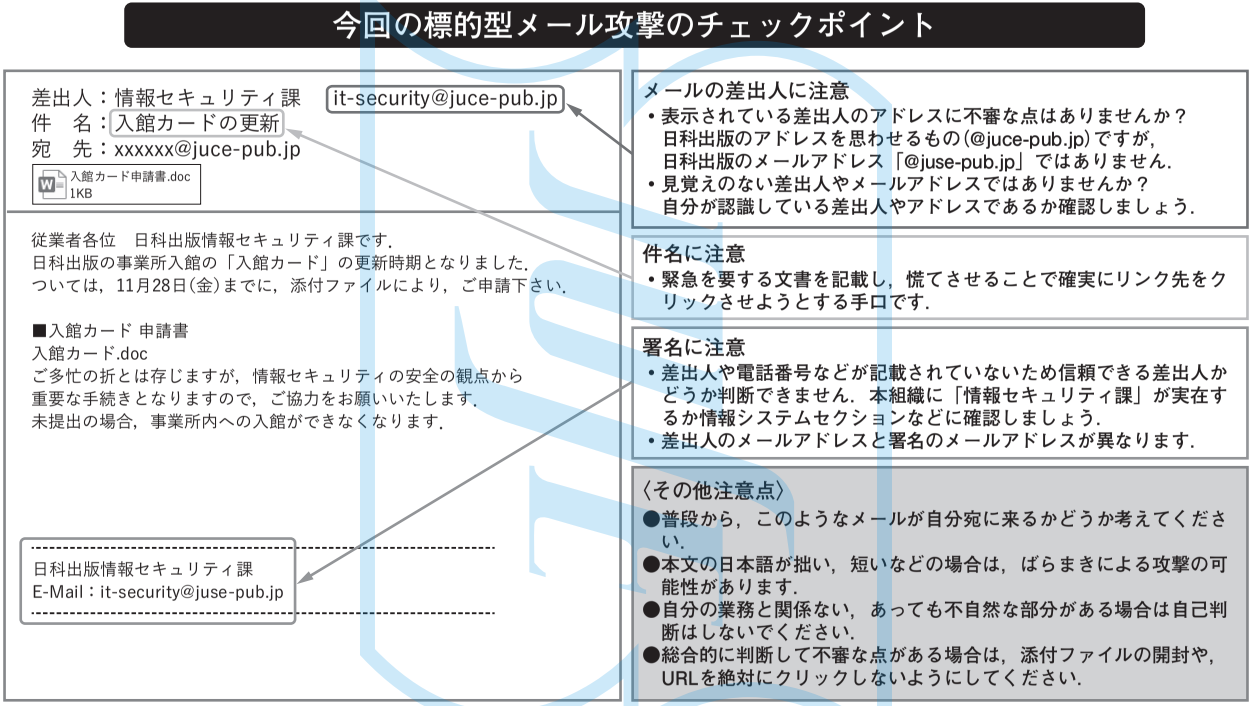
あたかも，緊急であるかのように装い，URL のクリックを誘導する．

第 3 のポイント：署名に注意

差出人をチェックする．

①　日科出版　情報セキュリティ課が存在するか．

→情報システム課は存在するが，情報セキュリティ課は存在しない．



図表 8.1　標的型メール攻撃のチェックポイント

索　引

［英数字］

accountability　86
APT　25
BCR　54
C&C サーバ　25
CPO　84
CVSS　79
CWE　68
　——TOP 25　68, 73
DPIA　52, 88
DPO　45
　——の職務　47
　——の選任の必要性　48
　——の地位　46
　——の役割　46
EU 個人データ保護指令　24
GDPR　24
　——の閾値分析　102, 105
　——の適用範囲　49
　——の罰則事例　44
　——リスク　31
OECD の 8 原則　26
OWSP　68
　——TOP 10　68, 69
PIA　88, 93
　——のプロセス　94
　——報告書　109
PII　93
　——主体　8
　——の影響度の基準　96
　——の発生頻度　98
　——のユースケース　105
P マーク　64
SDPC　53
URL 型　146

［ア　行］

アクセス権　28
暗号化　12
暗号キー　12
異議権　28
閾値分析　52, 98
一般化　18
一般データ保護規則　24, 26

［カ　行］

改正個人情報保護法　13, 24
仮名化　10, 11, 18
仮名データ　11
間接識別子　18
完全性および機密性の原則　28
管理者・処理者の義務　34
　——違反で制裁金を科す拠り所　35
管理者・処理者への処分　32
偽装メール　133
共通脆弱性評価システム　79
拘束的企業規則　54
個人情報　93
個人情報保護管理者　45
個人情報保護法　24
個人データ　8, 93
　——処理の原則　27
　——の自動処理にかかわる個人の保護

に関する条約　24
個人データ保護責任者　45
混合型　148

［サ　行］

最終責任　88
サイバー攻撃　4
——のパターン　127
サイバーセキュリティ　2
削除　18
——権　28
識別　19
識別行為の禁止　12, 14
自動化された決定及びプロファイリングについてのガイドライン　29
自動化された個人の判断に関する権利　28
十分性認定　52, 54
重法権　28
準同型暗号を用いた方式　21
情報セキュリティ管理責任者　45
シングルアウト　20
正確性の定義　27
制限権　28
制裁金　31
——の適用ルール　40
制裁の 4 原則　42
脆弱性　68
——診断サービス　81
——診断ツール　76
属性推定　19

［タ　行］

置換　18
訂正権　28
データ最小化の原則　27
データ主体　8
——の権利　28
——への権利侵害事項　37
データ処理原則への手続き違反　36
データポータビリティの権利　28
データ保護影響評価　52, 88
適法性，公平性および透明性の原則　27
添付ファイル型　146
統計処理　18
特定　19
匿名化　12
——のリスク　17
匿名加工情報　12, 61
匿名加工性　15
匿名性　12

［ハ　行］

パーソナルデータ　8
秘密計算　21
——の概要　20
秘密分散を用いた方式　21
紐　10
標準データ保護条項　53
標的型訓練の手順　146
標的型攻撃　25
標的型攻撃訓練メール　135
——のタイプ　146
標的型メール攻撃のチェックポイント　148
復号　12
不正メール　132
——の特長　148
プライバシー影響評価　88, 93

プライバシー責任者　*88*
プライバシーリスク評価　*107*
プライバシーリスク分析　*107*
プライバシーリスクマップ　*100, 101*
ペネトレーション　*81, 82*
——テスト　*82*
保管制限の原則　*27*
補完的ルールの適用範囲　*63*
保有個人データ　*56*

［マ　行］

マルウェア　*4*
身代金要求型ウイルス　*2*
メタデータ　*9*
目的限定の原則　*27*

［ヤ　行］

ユースケース　*106*
——分析　*106*
要配慮個人情報　*55*

［ラ　行］

ライフサイクル分析　*104, 106*
ランサムウェア　*2, 4, 116*
——の定義　*116*
——被害　*117*
——への対策　*129*
リスクマッピング　*52, 100*

［ワ　行］

忘れられる権利　*28*

著者紹介

畠中 伸敏（はたなか　のぶとし）

慶應義塾大学大学院工学研究科修士課程修了．工学博士．

キヤノン株式会社研究室長，東京情報大学大学院総合情報学研究科教授を経て，一般社団法人リスク戦略総合研究所理事長．

主著に『IoT 時代のセキュリティと品質』，『機密情報の保護と情報セキュリティ』，『環境配慮型設計』（いずれも，日科技連出版社），『予防と未然防止』（監修，日本規格協会），『情報心理』（編著，日本文教出版社），『情報セキュリティのためのリスク分析・評価』（編著，日科技出版社），『個人情報保護とリスク分析』（編著，日本規格協会），『ISO 9000 顧客満足システムの構築』（共著，日科技連出版社）など多数．

日本品質管理学会　品質技術賞（2000 年，2002 年），言語処理学会優秀発表賞（2002 年）．IEEE（終身会員），AAAI，ACM，情報処理学会（終身会員），人工知能学会，日本品質管理学会正会員．

サイバーセキュリティと個人情報保護

2025年12月26日　第1刷発行

著　者　畠中伸敏
発行人　戸羽節文

検印
省略

発行所　株式会社 日科技連出版社
〒151-0051　東京都渋谷区千駄ケ谷1-7-4
渡貫ビル
電話　03-6457-7875

Printed in Japan

印刷・製本　NS印刷製本㈱

ISBN 978-4-8171-9783-2

URL　https://www.juse-p.co.jp/