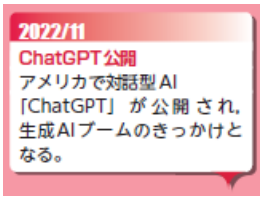
2025/1/30

実教出版「超スマート社会を生きるための　情報のセキュリティと倫理」（第 1 刷から第 2 刷への変更点）

第 1 刷から第 2 刷に増刷するにあたり，本書では下記の通り変更がございます。

箇所	1 刷	2 刷
p.7 ICT 関連技術サービス		※追加 
p.9　側注 カメラ撮影時のマナー	スマートフォンのカメラで，次のようなものを撮影したい時，場合によってはルール違反になることがあるため，注意しよう。	スマートフォンはカメラで気軽に撮影できるため，次の場面をはじめ，無断での撮影がルール違反となる場合でも安易に撮影してしまうことが多い。撮影したい場合は，関係者に許可を得てからにしよう。
p.19　側注 信憑性を判断する基準	情報の信ぴょう性とは，その情報の内容がどのくらい確かであると信用できるかということである。 ネット上の情報は，誰もが簡単に発信できるため，信ぴょう性の判断は，受信者側で行う必要がある。	情報の信憑性とは，その情報の内容が確かであると信用できる度合いのことをいう。 ネット上の情報（生成 AI から出力された情報も含む）は，誰かから安易に発信された情報も含まれているため，その信憑性の判断は，受信者の側で行われなくてはならない。
p.39　側注 プロバイダ責任制限法	プロバイダ責任制限法 この法律により，権利侵害情報に関し，プロバイダが保有する発信者の情報の開示を請求できる。開示請求を行う際，窓口として違法・有害情報相談センターがある。 （https://ihaho.jp/）	情報流通プラットフォーム対処法 （旧プロバイダ責任制限法） この法律により，SNS・電子掲示板の運営者やプロバイダに対して誹謗中傷記事の削除依頼や発信者の情報の開示を請求できる。それら削除依頼や開示請求に関する相談窓口として違法・有害情報相談センター(https://ihaho.jp/)がある。
p.41　側注 マイナンバー制度		※最下部に追加 マイナンバーカードの活用を進めるポータルサイトである「マイナポータル」では，税や社会保障などの機能を一元的に利用できる。

p.47　側注	**ビッグデータとAI** 人工知能(AI)はコンピュータで疑似的に人間の知能を再現し，問題の解決に役立てるしくみである。その実現のために，コンピュータは多くのデータをもとに人間の判断基準を再現していく。このため，データが多ければ多いほど精度は高くなる傾向にある。 ビッグデータの収集・活用はさまざまな問題を解決するために必要不可欠となりつつある。しかし，ビッグデータのもとになる情報には，個人情報が含まれている場合も多く，注意が必要である。 例えば，スマートフォンの位置情報の履歴などは，そのまま使用すると個人の行動履歴そのものが他人に知られることになってしまう。 ◎ビッグデータとして使える情報 ・電子マネーの利用履歴 ・共通ポイントの利用履歴 ・日々の天気 ・血圧，心拍数などバイタルサイン ・SNSでの発言　　など **連絡先データのアップロード** FacebookやLINEなどでは，電子メールアドレスや電話番号などの連絡先のデータをアップロードすることがある。アップロードした連絡先のデータの中に，別のユーザの連絡先が存在した場合，そのユーザどうしは知り合いである可能性が高い。「知り合いかも」に知り合いが表示されるのはこのためである。 しかし，自分の連絡先をアップロードされたくないという人がいることも考慮する必要がある。 また，知らないうちにアプリの設定により連絡先を共有してしまっていることがあるので，確認するとよい。	**ビッグデータと人工知能(AI)** 人工知能(AI)はコンピュータで疑似的に人間の思考プロセスを再現するしくみである。その実現のために，コンピュータは多くのデータをもとに人間の判断基準を再現していく。このため，データが多ければ多いほど精度は高くなる傾向にある。 学習データには，日々さまざまな種類や形式で蓄積されていく巨大なデータの集まりであるビッグデータが用いられる。 ビッグデータの収集・活用は，さまざまな問題を解決するために必要不可欠となりつつある。しかし，ビッグデータのもとになる情報には，例えば，スマートフォンの位置情報の履歴などのような個人情報が含まれている場合も多く，注意が必要である。 **生成AIと個人情報** 文章や画像，音声などのコンテンツを，プロンプトと呼ばれる命令により作り出すAIを生成AIという。 生成AIが作成するコンテンツはプロンプトに対して統計的に正しそうなものを組み合わせているので，正確な情報かどうかは利用者が判断する必要がある。また，生成AIにコンテンツを制作させる際に個人情報を入力すると，その個人情報も学習データとして取り込んでしまう場合があるので注意が必要となる。 **連絡先データのアップロード** Facebook（フェイスブック）やLINE（ライン）などでは，電子メールアドレスや電話番号などの連絡先データをアップロードすることがある。アップロードした連絡先データの中に，別のユーザの連絡先が存在した場合，そのユーザどうしは知り合いである可能性が高い。「知り合いかも」に知り合いが表示されるのはこのためである。 しかし，自分の連絡先をアップロードされたくないという人がいることも考慮する必要がある。 また，知らないうちにアプリの設定により連絡先を共有してしまっていることがあるので，確認するとよい。
p.53　側注 論文の引用と盗用	学問は，他人の成果を足掛かりに，自分の成果を加えることで発展してきた。このため，ほかの論文に引用された回数が多いほどよい論文とされている。そのため，引用することは必要だが，そのルールを守らない論文は厳しく非難される。 ノーベル賞の選定などでも，論文	学問は，他人の成果を足掛かりに，自分の成果を加えることで発展してきた。そのため，自分の論文には先行研究の論文から引用したものであることを明記し，その上で自分の研究の成果を記載する。論文の引用回数が多いということは，その論文の学術的価値が高いとみなされる。し

	の引用回数は大きく評価されている。引用回数が多いということは，その論文に述べられている内容に学術的価値があり，その実験結果や理論をもとに新しい学問分野が発展していることを示す。	かし，他人の研究成果を自分の成果のように記載することは盗用であり，厳しく非難される。 提出されたレポートが他人のWeb サイトから盗用したものでないかをチェックする機能を提供しているオンラインサービスもある。この機能を利用すると，レポートのどの部分が，どこのサイトのどの部分と共通しているかを示すことができ，盗用がすぐわかる。盗用は，自分への信頼を損ねる行為であることを知っておきたい。
p.53　側注 盗用チェック機能		削除
p.53　側注		※追加 **生成AIでの論文作成** 自分の考えを文章にまとめたいときや読みやすい文章を作りたいとき，生成AIは便利なツールとして活用できる。 自分の考えを箇条書きしたものや文章の下書きを生成AIに入力すれば，完成された文章が出力される。また，生成AIは文章だけでなくグラフ作成なども行える。 しかし，出来上がった文章やグラフが正しいかどうかは，利用する本人が責任を持つ必要がある。なぜなら，作成した文章の信憑性やグラフの妥当性の保証は，生成AIを利用した本人にあるためである。
p.55 関連キーワード		※追加 パスキー認証
p.55　側注 ワンタイムパスワード	タイトル： ワンタイムパスワード	タイトル： ワンタイムパスワード／パスキー ※文章追加 また，パスワードを入力する代わりに顔や指紋などの生体認証を利用してログインするパスキーも普及している。パスワードを使用しないため，ユーザの負担軽減と，フィッシング詐欺(→p.37,71)などの防止につながっている。
p.67 関連キーワード	SSL/TSL	TLS
p.67　側注	タイトル： SSL/TLS のしくみ	タイトル： TLS のしくみ

	文章： 　インターネット上で，データを迅速に暗号化し，安全にデータをやり取りするために一般的に使われるものとして，SSL/TLS（Secure Socket Layer/Transport Layer Security）がある。これは，共通鍵暗号方式と公開鍵暗号方式を組み合わせた暗号方式である。それぞれの方式の特徴を組み合わせて，安全で，高速な処理が可能となっている。	文章： 　インターネット上で，データを迅速に暗号化し，安全にデータをやり取りするために一般的に使われるものとして，TLS（Transport Layer Security）がある。 　なお，TLS は以前使われていた SSL（Secure Sockets Layer）の脆弱性を解決した暗号方式である。
p.73 4　音楽著作権の包括契約 5　ゲーム実教動画の著作権	削除	
p.73 ページ下部	※追加 **04 生成 AI と個人情報・著作権の問題** **1 生成 AI と個人情報** 　生成 AI を利用する際に入力するプロンプト（命令）に個人情報に類するデータが含まれる場合，あらかじめ本人の同意を得る必要があります。もし許諾を得ることなく行った場合，個人情報保護法の違反になる可能性があります。 **2 生成 AI と著作権** 　生成 AI は，大量の著作物等のデータを学習し，学習したデータを組み合わせることにより，文章や画像等のコンテンツを生成するものです。コンテンツを生成する際，元となるデータが著作権で保護されたものである可能性があり，生成されたコンテンツが著作物に酷似している場合，著作権侵害の可能性がでてきます。 　また，AI による生成物の著作権を誰が所持するかに関しては，法的に未解決の部分が多く，課題となっています。	
p.80　02 SNS の「いいね」 3 段落目と 4 段落目の間		p.81　4　「より豊かなコミュニケーションをめざして」から以下の文章移動： 自分をよりよく見せようとしたり，「いいね」を欲しがったりする背景には，自己承認欲求の高まりがあるといわれています。自分に自信をもてなかったり，生活に満足感をもつことができなかったりといったことが，自己承認欲求が高くなる一因といわれています。
p.81　03 SNS による誹謗中傷 11 行目と 12 行目の間		※追加 　また，あるプロスポーツ選手のとある試合でのプレーに関して，一般的に「ヤジ」と呼ばれるような心無い言葉や直接的な暴力行為を示唆するような言葉が多数投稿されました。これに心を痛めた同選手は，発信者情報の開示請求申し立てを行い，申し立てが認められることになりました。このことによ

		り，同選手と投稿した人との間では示談が成立しました。このような行為は民事だけでなく刑事事件として扱われることもあります。
p.87　02 ネット依存症の予防 文章の 2 行目	ネット上のゲームやコミュニケーションに過度にのめり込んで	ネット上の動画視聴やゲーム，コミュニケーションに過度にのめり込んで
p.89 個人情報保護法 04	学校に設置されている共用パソコン	共用パソコン
p.90 プロバイダ責任制限法　01	インターネット上の Web ページや電子掲示板などに掲載された情報で名誉毀損や著作権侵害があったとき，プロバイダや掲示板管理者が負う損害賠償責任の範囲や，情報発信者の情報の開示を請求する権利について定めた法律のことです。	Web ページや電子掲示板だけでなく，SNS などの大規模プラットフォームを対象として，そこに書かれた情報が名誉毀損や著作権侵害にあたるとき，プロバイダや電子掲示板の管理者，SNS の運営者が負う損害賠償責任の範囲や，発信者情報の開示請求の権利などについて定められた法律のことです。
p.90 プロバイダ責任制限法　02	加害者が誰かということがわかっていれば，直接クレームをいったり訴訟を起こしたりできますが，インターネットの場合には情報の発信者が不明であることが多く，一般的にプロバイダにとっても通信の秘密を守るために発信者情報を明らかにはできません。そこで，明らかに権利が侵害されたときや，開示請求者が損害賠償請求をするのに必要な場合には，プロバイダに対し発信者情報を開示請求できるという権利です。	インターネットの場合には情報の発信者が不明であることが多く，一般的にプロバイダにとっても通信の秘密を守るために発信者情報を明らかにはできません。そこで，明らかに権利が侵害されたときは，SNS や電子掲示板などの運営者に対して IP アドレスの開示請求やプロバイダに対して契約者情報の開示請求ができるという権利です。
p.90 プロバイダ責任制限法　03	インターネットの掲示板に私の誹謗中傷が書かれた記事を見つけました。削除するにはどうすればいいですか？	SNS に私の誹謗中傷が書かれているのを見つけました。削除するにはどうすればいいですか？
	その掲示板を運営する管理者もしくはプロバイダに連絡を取り削除依頼をしてください。	その SNS の運営者もしくはプロバイダに連絡を取り，削除依頼をしてください。
p.93　左段 プロバイダ責任制限法	タイトル：プロバイダ責任制限法 Web ページや電子掲示板など	※タイトル：情報流通プラットフォーム対処法 Web ページや電子掲示板，SNS など
p.93　右段 HTTPS	SSL で暗号化された Web ページ	暗号化された Web ページ
p.93　右段 人工知能（AI）	コンピュータで再現する仕組み。	コンピュータなどで再現する仕組み。
p.93　右段 人工知能（AI）		※後ろに追加

		20 **生成AI** 文章や画像，音声などのコンテンツを，プロンプトと呼ばれる命令により作り出すAI。
p.93　右段 ビッグデータ	日々さまざまなデータが蓄積されていく	p.94 に移動 日々さまざまな種類や形式で蓄積されていく
p.94　右段 認証　と　パスワードの間		※追加 24 **パスキー認証** パスワードを入力する代わりに，顔や指紋などの生体認証を利用してログインする方法。
p.95　左段	可用性 完全性 機密性	削除
p.95　右段 不正アクセス禁止法	なお，正式名称は，「不正アクセス行為の禁止に関する法律」である。	削除
p.95　右段 SSL/TSL	SSL/TSL 共通鍵暗号方式と公開鍵暗号方式を組み合わせたハイブリッド暗号方式である。インターネットの暗号化通信でよく利用される。Secure Sockets Layer / Transport Layer Security の略。	TLS インターネット上で，データを迅速に暗号化し，安全にデータをやり取りするために使われる暗号通信技術である。Transport Layer Security の略。 なお，TLS は以前使われていた SSL（Secure Sockets Layer）の脆弱性を解決している。

以上

実教出版「超スマート社会を生きるための　情報のセキュリティと倫理」第１刷用補遺

本書発行時からの社会情勢等の変化に伴い，下記の変更がございます。

１刷	２刷
Twitter	X（旧 Twitter）
プロバイダ責任制限法	情報流通プラットフォーム対処法
ケータイ	スマホ
GPS	GNSS 位置情報サービス
ツイート	ポスト