

セキュリティ関連法規(Security-Related Laws and Regulations)

不正アクセスやサイバー犯罪の防止に関する法律

不正アクセス禁止法(Unauthorized Computer Access Law):コンピュータやネットワークへの無断アクセスを防止する法律

不正アクセス禁止法では、次の 5 つの行為が禁止されている:

- ① 不正にアクセスすること
- ② 他人の認証情報を第三者に不正に提供(教える)すること
- ③ 不正な目的で他人の認証情報を入手すること
- ④ 不正な目的で他人の認証情報を保管すること
- ⑤ 管理者を装うなどして、利用者をだまし(誤認させて)、認証情報を要求すること

不正指令電磁的記録に関する罪(Crime of Unauthorized Commands Involving Electromagnetic Records):

コンピュータウイルスなど、悪意のあるプログラムを作成・配布する行為を禁止する刑法上の罪

サイバーセキュリティ全般に関する法律・ガイドライン

サイバーセキュリティ基本法(Basic Act on Cybersecurity):国や企業がサイバーセキュリティ(Cybersecurity)を確保するための基本的な枠組みを定めた法律

日本政府は「サイバーセキュリティ戦略本部」と「NISC(内閣サイバーセキュリティセンター)」を設置

規定内容:政府機関や重要インフラのセキュリティ確保、民間企業や教育機関のセキュリティ強化、サイバー攻撃への緊急対応、国際協力の推進

サイバーセキュリティ経営ガイドライン(Cybersecurity Management Guidelines):

企業がサイバーセキュリティ対策を適切に実施するためのガイドライン → 経営者が認識すべき原則や取り組むべき項目が書かれている

個人情報保護に関する法律

個人情報保護法(Personal Information Protection Law):個人情報を保護し、無断で使用されないようにするための法律

利用目的を(合理的な範囲で)変更した場合 → 本人に通知、又は、公表をする必要がある

要配慮個人情報:個人のプライバシーに重大な影響を与える情報

例:人種、宗教、信条、社会的身分、病歴、犯罪歴など

GDPR(General Data Protection Regulation):

欧州連合(EU)で適用される個人データ保護のための厳しい規則

GDPR の適用範囲

	EU 内の事業者	EU 外の実業家
EU 内に商品・サービスを提供	適用あり	適用あり
EU 外に商品・サービスを提供	適用あり	適用なし

アクセス制御とセキュリティ機能に関する概念

アクセス制御機能(Access Control Function):コンピュータやシステムへのアクセスを制限する機能(例:IDとパスワードを使ってログインする機能)

オプトイン(Opt-in):デフォルト(初期設定)で未同意(default consent not given)、同意するためにアクションが必要

オプトアウト(Opt-out):デフォルト(初期設定)で同意済み(default consent given)、拒否するためにアクションが必要

セキュリティ関連法規 (Security-Related Laws and Regulations)

不正アクセスやサイバー犯罪の防止に関する法律

不正アクセス禁止法 (Unauthorized Computer Access Law): コンピュータやネットワークへの無断アクセスを防止する法律

不正アクセス禁止法では、次の5つの行為が禁止されている:

- ① 不正にアクセスすること
- ② 他人の認証情報を第三者に不正に提供(教える)すること
- ③ 不正な目的で他人の認証情報を入手すること
- ④ 不正な目的で他人の認証情報を保管すること
- ⑤ 管理者を装うなどして、利用者をだまし(誤認させて)、認証情報を要求すること

不正指令電磁的記録に関する罪 (Crime of Unauthorized Commands Involving Electromagnetic Records):

コンピュータウイルスなど、悪意のあるプログラムを作成・配布する行為を禁止する刑法上の罪

サイバーセキュリティ全般に関する法律・ガイドライン

サイバーセキュリティ基本法 (Basic Act on Cybersecurity): 国や企業がサイバーセキュリティ (Cybersecurity) を確保するための基本的な枠組みを定めた法律

日本政府は「サイバーセキュリティ戦略本部」と「NISC (内閣サイバーセキュリティセンター)」を設置

規定内容: 政府機関や重要インフラのセキュリティ確保、民間企業や教育機関のセキュリティ強化、サイバー攻撃への緊急対応、国際協力の推進

サイバーセキュリティ経営ガイドライン (Cybersecurity Management Guidelines):

企業がサイバーセキュリティ対策を適切に実施するためのガイドライン → 経営者が認識すべき原則や取り組むべき項目が書かれている

個人情報保護に関する法律

個人情報保護法 (Personal Information Protection Law): 個人情報を保護し、無断で使用されないようにするための法律

利用目的を(合理的な範囲で)変更した場合 → 本人に通知、又は、公表をする必要がある

要配慮個人情報: 個人のプライバシーに重大な影響を与える情報

例: 人種、宗教、信条、社会的身分、病歴、犯罪歴など

GDPR (General Data Protection Regulation):

欧州連合 (EU) で適用される個人データ保護のための厳しい規則

アクセス制御とセキュリティ機能に関する概念

アクセス制御機能 (Access Control Function): コンピュータやシステムへのアクセスを制限する機能 (例: IDとパスワードを使ってログインする機能)

オプトイン (Opt-in): デフォルト (初期設定) で未同意 (default consent not given)、同意するためにアクションが必要

オプトアウト (Opt-out): デフォルト (初期設定) で同意済み (default consent given)、拒否するためにアクションが必要

GDPR の適用範囲

	EU内の事業者	EU外の事業者
EU内に商品・サービスを提供	適用あり	適用あり
EU外に商品・サービスを提供	適用あり	適用なし

セキュリティ関連法規 (Security-Related Laws and Regulations)

不正アクセスやサイバー犯罪の防止に関する法律

:コンピュータやネットワークへの無断アクセスを防止する法律

不正アクセス禁止法では、次の5つの行為が禁止されている:

- ① 不正に すること
- ② 他人の認証情報を第三者に不正に すること
- ③ 不正な目的で他人の認証情報を すること
- ④ 不正な目的で他人の認証情報を すること
- ⑤ を装うなどして、利用者をだまし(誤認させて)、認証情報を要求すること

不正指令電磁的記録に関する罪 (Crime of Unauthorized Commands Involving Electromagnetic Records):

コンピュータウイルスなど、悪意のあるプログラムを作成・配布する行為を禁止する刑法上の罪

サイバーセキュリティ全般に関する法律・ガイドライン

:国や企業がサイバーセキュリティ (Cybersecurity) を確保するための基本的な枠組みを定めた法律

日本政府は「サイバーセキュリティ戦略本部」と「NISC (内閣サイバーセキュリティセンター)」を設置

規定内容: 政府機関や重要インフラのセキュリティ確保、民間企業や教育機関のセキュリティ強化、サイバー攻撃への緊急対応、国際協力の推進

サイバーセキュリティ経営ガイドライン (Cybersecurity Management Guidelines):

企業がサイバーセキュリティ対策を適切に実施するためのガイドライン → が認識すべき原則や取り組むべき項目が書かれている

個人情報保護に関する法律

:個人情報を保護し、無断で使用されないようにするための法律

利用目的を (合理的な範囲で) 変更した場合 → 本人に通知、又は、公表をする必要がある

:個人のプライバシーに重大な影響を与える情報

例: 人種、宗教、信条、社会的身分、病歴、犯罪歴など

GDPR の適用範囲

	EU内の事業者	EU外の事業者
EU内に商品・サービスを提供	適用あり	適用あり
EU外に商品・サービスを提供	適用あり	適用なし

欧州連合 (EU) で適用される個人データ保護のための厳しい規則

アクセス制御とセキュリティ機能に関する概念

機能 (Access Control Function): コンピュータやシステムへのアクセスを制限する機能 (例: IDとパスワードを使ってログインする機能)

: デフォルト (初期設定) で未同意 (default consent not given)、同意するためにアクションが必要

: デフォルト (初期設定) で同意済み (default consent given)、拒否するためにアクションが必要

Security-Related Laws and Regulations

Laws Against Unauthorized Access and Cybercrime

Unauthorized Computer Access Law: Prevents unauthorized access to computers and networks. It prohibits:

- 1. Unauthorized access.
- 2. Illegally providing someone else’s authentication information.
- 3. Obtaining authentication information for malicious purposes.
- 4. Storing authentication information for malicious purposes.
- 5. Pretending to be an administrator to trick users into providing authentication information.

Crime of Unauthorized Commands Involving Electromagnetic Records: Prohibits the creation and distribution of malicious programs like computer viruses.

Cybersecurity Laws and Guidelines

Basic Act on Cybersecurity: Establishes a framework for ensuring cybersecurity by the government and businesses. The Japanese government created the "Cybersecurity Strategy Headquarters" and "NISC" under this law.

- Provisions include: securing government agencies and critical infrastructure, strengthening cybersecurity in businesses and education, responding to cyberattacks, and promoting international cooperation.

Cybersecurity Management Guidelines: Provide principles and actions for companies to implement effective cybersecurity measures.

Personal Information Protection Laws

Personal Information Protection Law: Protects personal information and prevents unauthorized use. Changes in the purpose of data use require notification or public announcement.

- Sensitive Personal Information: Includes data with significant privacy impact (e.g., race, religion, social status, medical history, criminal history).

GDPR (General Data Protection Regulation):
Strict data protection regulations applicable within the EU.

Access Control and Security Concepts

- Access Control Function:** Limits system access (e.g., using an ID and password).
- Opt-in:** Default consent is not given; action required to agree.
- Opt-out:** Default consent is given; action required to refuse.

GDPR Applicability

	EU-based Businesses	Non-EU Businesses
Providing goods/services within the EU	Applicable	Applicable
Providing goods/services outside the EU	Applicable	Not Applicable