A-4.
サイバー攻撃への対策

昭和女子大学
中田　亮太郎

このセッションの目標

サイバー攻撃の事前対策として、どのような技術があるかを理解する。また、個人情報保護法やGDPRなど、法的側面を考慮したシステム/ユーザーレベルでの対策を理解する。

▼

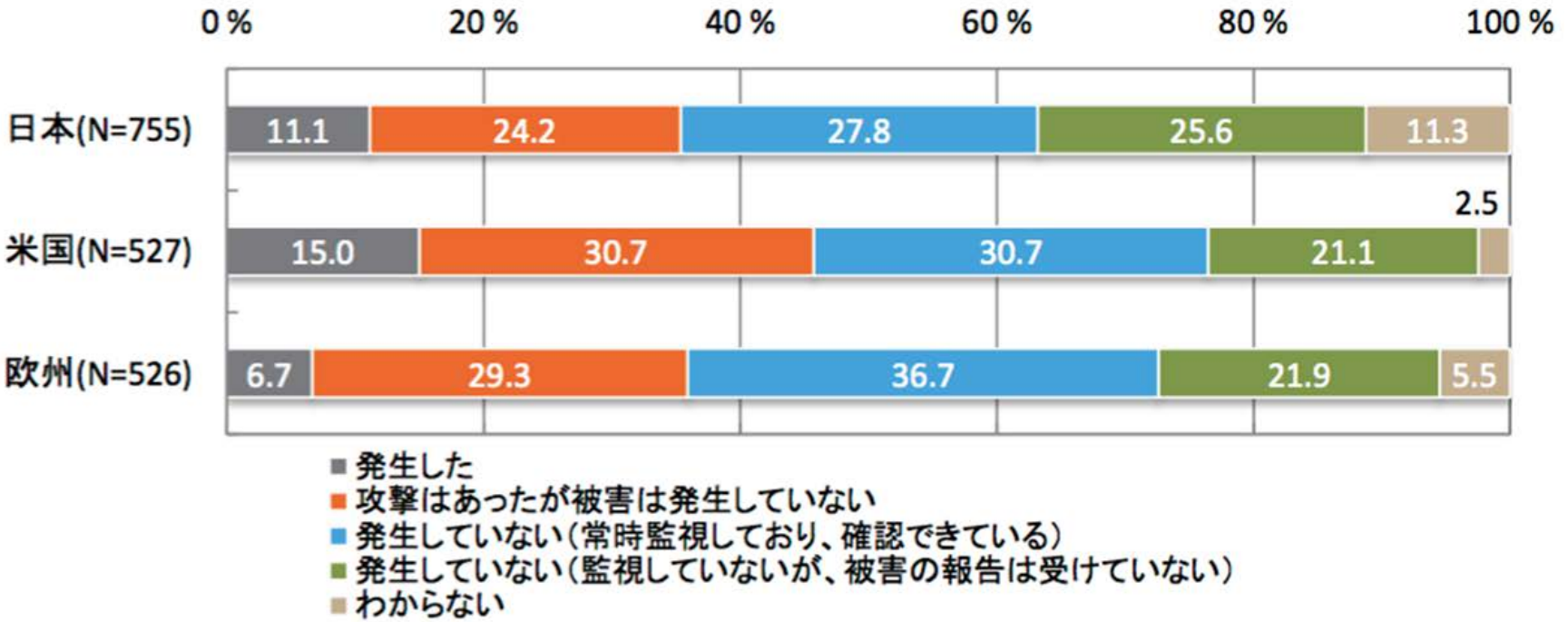
① 最新のレギュレーションの内容や動向を把握し、自校での対応や改善点を見出す。

② 技術的対策例を通し、サイバー攻撃への具体的な事前対策を考察・実施できるようにする。

サイバー攻撃の状況

サイバー攻撃の状況

- サイバー攻撃被害経験の有無

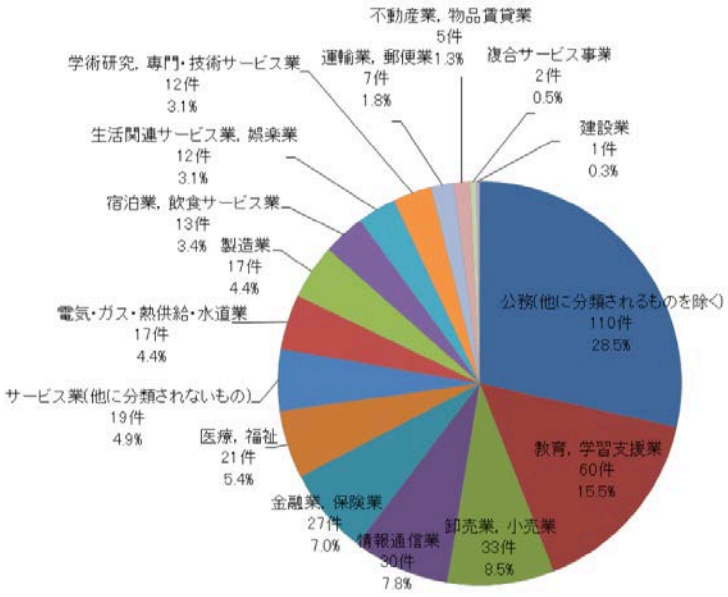


出典：IPA 企業のCISOやCSIRTに関する実態調査2017 調査報告書

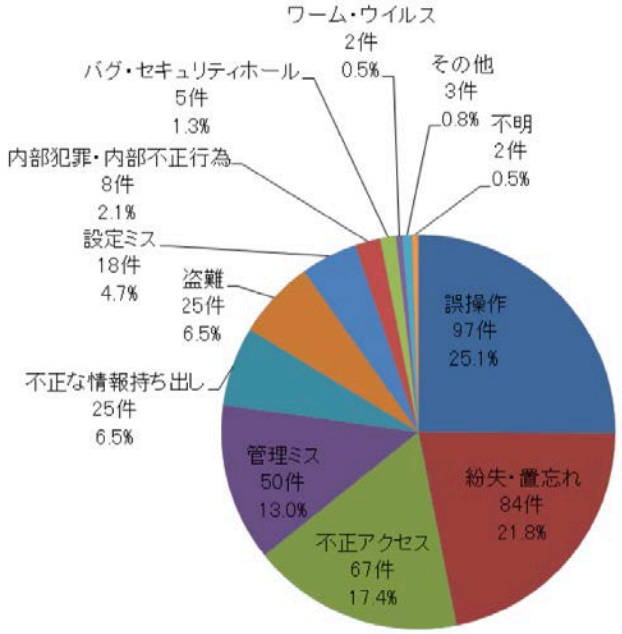
サイバー攻撃の状況

- 国内のインシデント状況

業種別漏えい件数



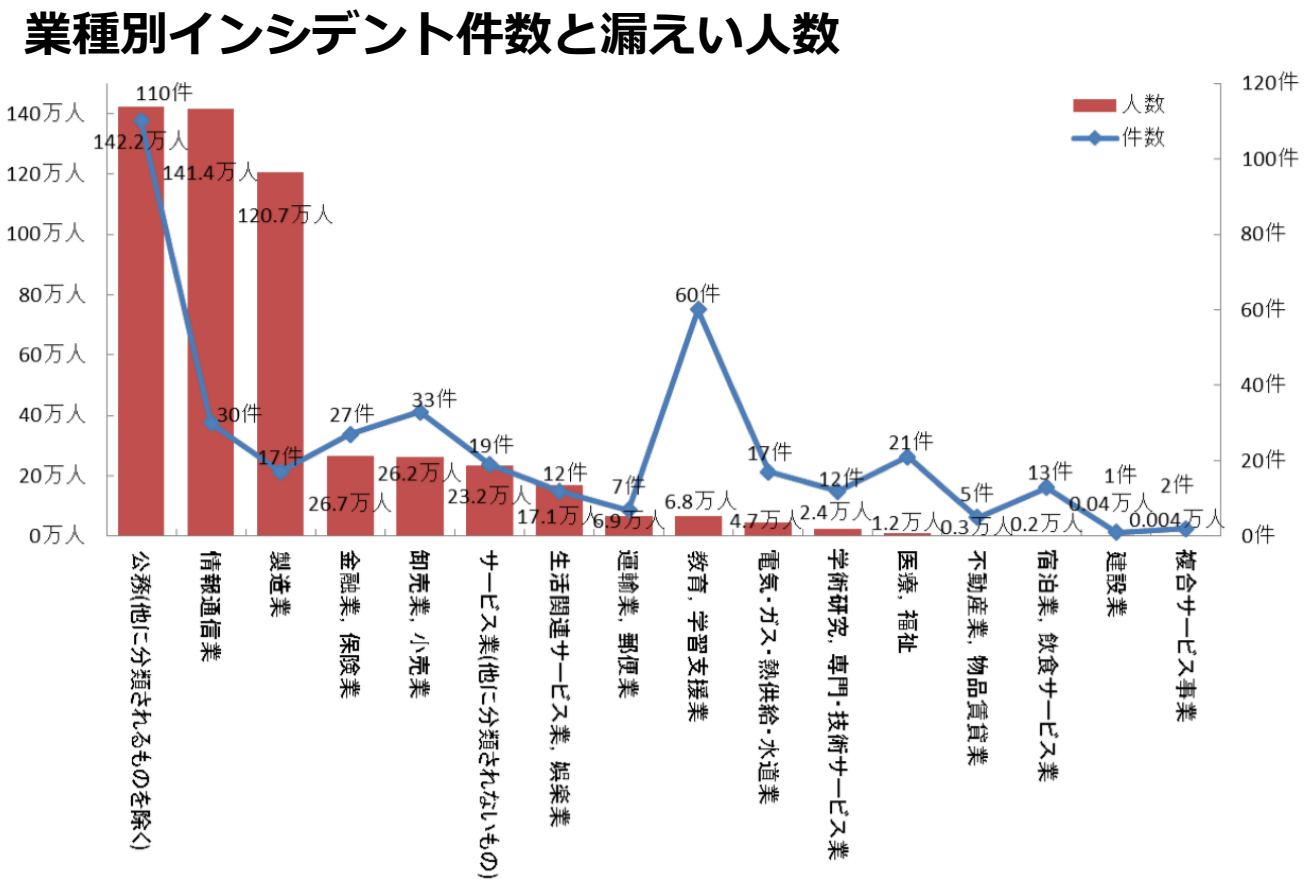
漏えい原因



出典：JNSA2017年情報セキュリティインシデントに関する調査報告書

サイバー攻撃の状況

- 国内のインシデント状況



出典：JNSA2017年情報セキュリティインシデントに関する調査報告書

公益社団法人　私立大学情報教育協会

サイバー攻撃の状況

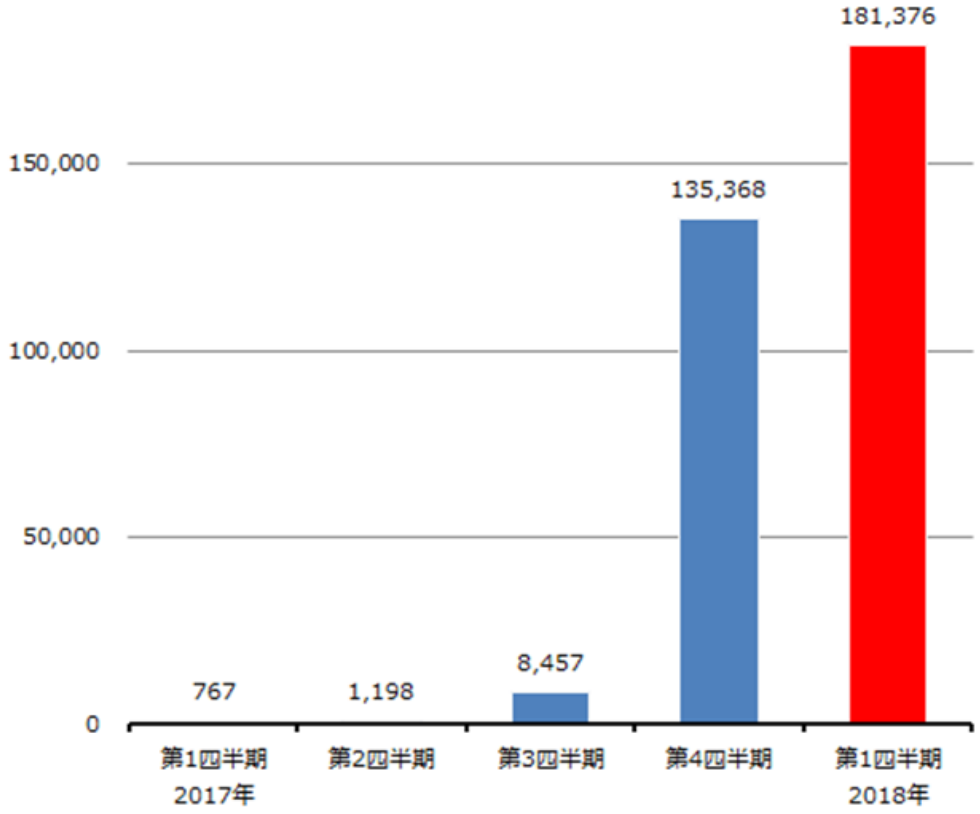
- 大学での不正アクセス等被害事例

時期	大学名	内容
2018.5	T大学	不正アクセスで迷惑メールの踏み台に
2018.4	K大学	不正アクセスで迷惑メール送信
2018.3	C大学	PCやサーバがランサムウェアに感染
2018.1	N大学	不正アクセスでウェブ改ざん
2017.12	O大学	管理者アカウント奪われ情報漏洩
2017.5	H大学	不正アクセスで情報搾取
2017.1	N大学	公開用サーバが不正アクセスの踏み台に

「セキュリティ」と「利便性」を両立できる対策ができるか？
教育・研究は大義名分となるのか？

サイバー攻撃の状況

- 金銭的利益を狙ったものが急増



国内コインマイナー検出の推移

出典：トレンドマイクロ2018第1四半期セキュリティラウンドアップ

法律と実施すべき対策

関連する法律

- 代表的な情報セキュリティ関連の法律

名称	内容	備考
刑法	犯罪と刑罰に関する法律	電子計算機損壊等業務妨害罪 電磁的記録不正作出及び供用罪 電子計算機使用詐欺罪 不正指令電磁的記録に関する罪　等
サイバーセキュリティ基本法	サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を規定	
著作権法	著作物などに関する著作者等の権利を保護するための法律	
電気通信事業法	「通信の秘密」など、電気通信の健全な発達と国民の利便の確保を図るための法律	
電子署名法	一定の条件を満たす電子署名が手書き署名や押印と同等とする認証制度などを規定	正式名称： 電子署名及び認証業務に関する法律
電波法	無線局の開設や秘密の保護などについての取り決めが規定	
特定電子メール法	いわゆる迷惑メール防止法。利用者の同意を得ずに広告、宣伝等を目的としたメールを送信する際の規定	正式名称： 特定電子メールの送信の適正化等に関する法律
不正アクセス禁止法	不正アクセス行為や、不正アクセス行為につながる識別符号の不正取得・保管行為等を禁止する法律	正式名称： 不正アクセス行為の禁止等に関する法律

関連する法律

サイバーセキュリティ基本法

2015年1月15日全面施行

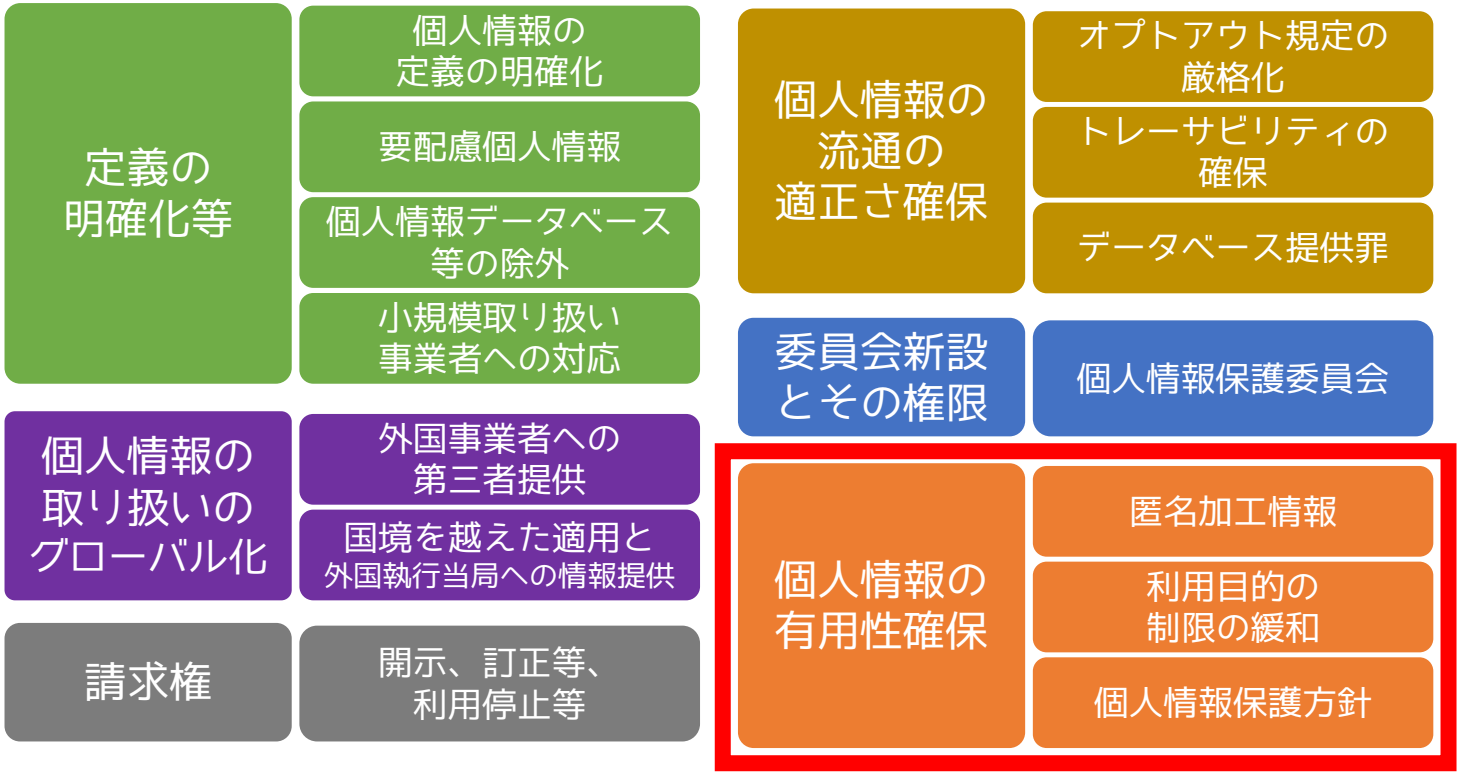
電子情報についての安全性や信頼性が確保され、維持されること

- 国家 地方公共団体の責務
  - 行政面の果たすべき責務や、重要インフラ事業者、IT事業者、一般事業者の果たすべき責務が定められた
- 企業の責務
  - 研究の促進と人材の育成に力を入れることを求めた
- 教育機関の責務
  - 国民に対し、理解を深めることを求めた
- 国民の努力
  - 戦略を定め、官房長官を本部長とする戦略本部を設置した
- 戦略本部の設置

関連する法律

■ 改正個人情報保護法

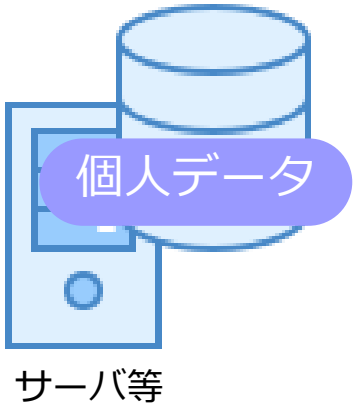
2017年5月30日全面施行



個人の特定性を下げることで、データの利活用を可能とする枠組みを設けた

実施すべき対策

- 個人情報保護法で必要な安全管理措置



改正個人情報保護法

19条 データ内容の正確性の確保
20条 安全管理措置
21条 従業者の監督
22条 委託先の監督
23条 第三者提供の制限
24条 外国にある第三者への提供の制限
25条 第三者提供に係る記録の作成等
26条 第三者提供を受ける際の確認等

8. 講ずべき安全管理措置の内容

8-1 基本方針の策定
8-2 個人データの取り扱いに係る規律の整備
8-3 組織的安全管理措置
8-4 人的安全管理措置
8-5 物理的安全管理措置
8-6 技術的安全管理措置

実施すべき対策

■ 安全管理措置の内容と対策手法の例

8 講ずべき安全管理措置の内容			手法の例
8-1	基本方針の策定		
8-2	個人データの取り扱いに関する規律の整備		
8-3	組織的安全管理措置	(1)組織体制の整備	ログイン実績・アクセスログ等
		(2)個人データの取り扱いに関わる規律に従った運用	
		(3)個人データの取り扱い状況を確認する手段の整備	
		(4)漏えい等の事案に対応する体制の整備	
		(5)取り扱い状況の把握及び安全管理措置の見直し	定期的に自ら行う点検又は他部署等による監査
8-4	人的安全管理措置	(1)従業者の教育	
8-5	物理的安全管理措置	(1)個人データを取り扱う区域の管理	
		(2)機器及び電子媒体等の東南東の防止	
		(3)電子媒体等を持ち運ぶ場合の漏えい等の防止	暗号化
		(4)個人データの削除及び機器、電子媒体等の廃棄	
8-6	技術的安全管理措置	(1)アクセス制御	アクセス制御
		(2)アクセス者の識別と認証	認証
		(3)外部からの不正アクセス等の防止	ログ等の定期的な分析
		(4)情報システムの使用に伴う漏えい等の防止	通信経路・内容の暗号化

実施すべき対策

■ 技術的安全管理措置の詳細

8-6 技術的安全管理措置			対策方法の例
(1)	アクセス制御	担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない。	• 個人情報データベース等を取り扱うことのできる情報システムを限定する。 • 情報システムによってアクセスすることのできる個人方法データベース等を限定する。 • ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。
(2)	アクセス者の識別と認証	個人データを取り扱う情報システムを使用する従業者が正当なアクセス権を有するものであることを、識別した結果に基づき認証しなければならない。	• ユーザーID • パスワード • 磁気/ICカード　等
(3)	外部からの不正アクセス等の防止	個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。	• 情報システムと外部ネットワークの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 • 情報システムおよび機器にセキュリティ対策ソフトウェア等（ウィルス対策ソフトウェア等）を導入する。 • 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 • ログ等の定期的な分析により、不正アクセス等を検知する。
(4)	情報システムの使用に伴う漏えい等の防止	情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。	• 情報システムの設計時に安全性を確保し、継続的に見直す。（情報システムの脆弱性を突いた攻撃への対策を講じることも含む） • 個人データを含む通信の経路または内容を暗号化する。 • 移送する個人データについて、パスワード等による保護を行う。

実施すべき対策

- 情報セキュリティ部門が考慮・対策すべき内容

対策	内容
ID管理・認証	ID作成と管理・認証・多要素認証・段階的認証・シングルサインオン・フェデレーション
権限管理	役割と権限の整理・ロールモデル構築・アクセス権設定・特権管理
アクセス制御	制御方式・Windowsアクセス制御・データベース・アプリケーション・サービス
ネットワーク管理	プライベート・グローバル・セグメント・DMZ・ACL・FW・無線LAN・IPv6・SDN
ソフトウェア管理 脆弱性対策	導入・維持・OS・OSS・パッケージ・独自開発・脆弱性管理・情報収集
サーバ/クライアント管理	マルウェア・エンドポイント対策・ゲートウェイ対策・感染時対応
データ保護/暗号化	共通鍵・公開鍵・SSL・TLS・利用ポリシー・電子署名・PKI
データ廃棄	データ消去・データ廃棄・記録媒体廃棄・リサイクル
物理的保護	施設設備の保護・サーバやネットワーク機器の保護・PCやIoT機器の保護・落雷対策

実施すべき対策

- 組織全体で取り組む情報セキュリティ

情報セキュリティガバナンス –内部統制と社会的責任–

情報セキュリティマネジメント

情報システムを守る

システム部門
技術的対策
不正アクセス防止
ウィルス対策

情報を守る

組織全体で取り組む
情報セキュリティ
（人的、物理的、
技術的、管理的）

組織内の情報及び情報システムの信頼性・安全性の確保

組織を守る・維持する

経営を守る

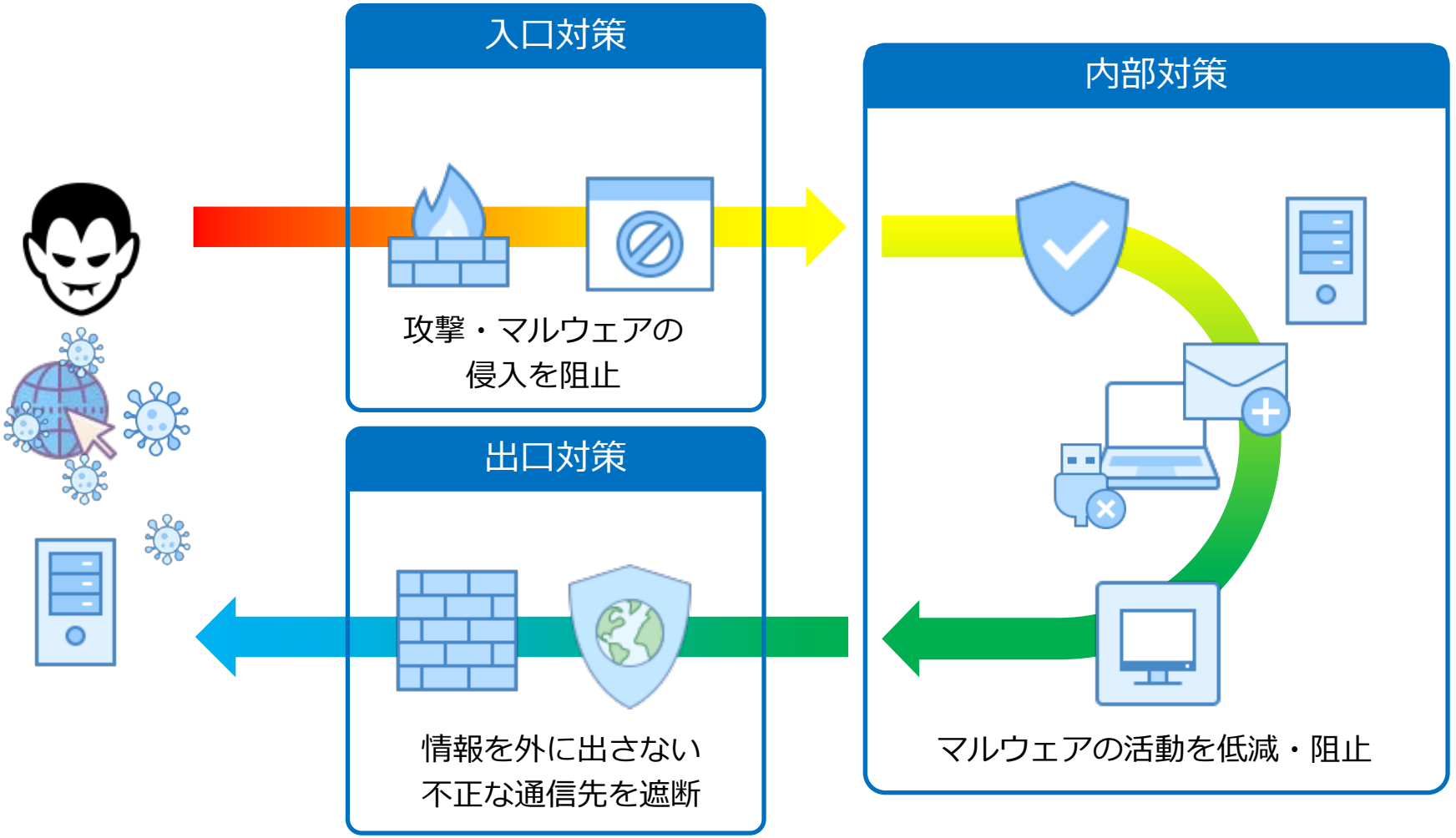
法令遵守や社会的責任などの観点も踏まえた情報セキュリティ対策への取り組み

内部統制の確立

多層防御

多層防御

- 侵入を前提とした対策



多層防御

- 入口対策（侵入対策）

分類	対策例	残存リスク
ネットワーク	IPS/IDSにより攻撃トラフィックを検知・遮断	0-day攻撃
	次世代ファイアウォール／サンドボックス型検知システム等による未知のマルウェア検知	検知漏れ
	送信ドメイン認証による不正メールの遮断	認証可能なドメインが限定されている

多層防御

■ 内部対策（拡大対策）

分類	対策例	残存リスク
ネットワーク	パッチマネジメント強化による脆弱性対策	0-day攻撃
	パスワード管理強化によるマルウェア感染拡大防止	脆弱なパスワード
	外部記録媒体の利用制限によるマルウェア感染防止	正規媒体からの感染
	脆弱性緩和ツール等の適用	脆弱性を突かない攻撃
	振る舞い検知型ソフトウェア等の導入	検知漏れ
	起動プログラム制限	導入が困難なケース
LAN/WAN	不正端末の接続防止	正規端末からの攻撃
	IPS/IDSにより攻撃トラフィックを検知・遮断	0-day攻撃
サーバー	アクセス制御の強化	正当なアクセス権限を利用した攻撃
	サーバ要塞化による脆弱性の削減	脆弱性対策漏れ
データ	データの暗号化	解読された状態での漏えい

多層防御

- 出口対策（漏えい対策）

分類	対策例	残存リスク
ネットワーク	通信先URL/IPアドレスのフィルタリング	フィルタリング漏れ
	大量の外向け通信の制限	少量の通信による漏えい
	IPS/IDSによる不正トラフィックの検知／遮断	0-day攻撃

多層防御

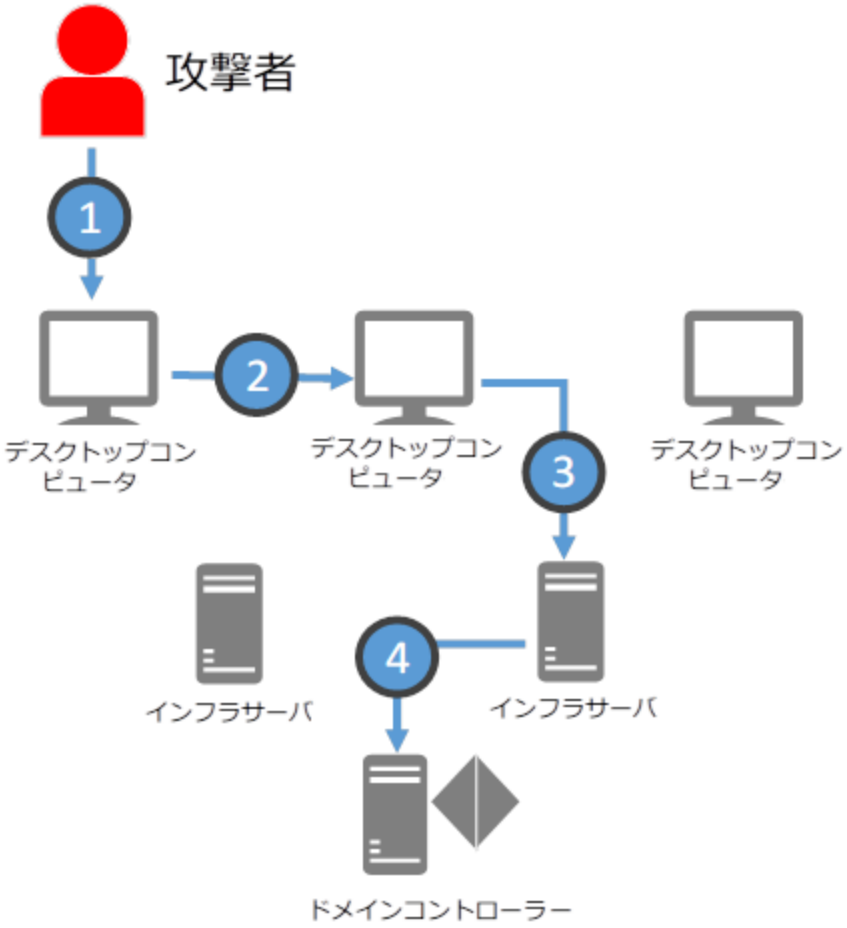
- 総合的対策（技術的対策および教育・体制強化）

分類	対策例	残存リスク
ユーザー教育	教育によるエンドユーザの意識向上	詐欺的手法による高度な攻撃
	疑似標的型メール送信による訓練	新しい手口等による攻撃
統合監視	各種ログ収集・監視強化	
インシデント対応体制	インシデント発生の迅速な対応体制の構築	

具体的対策例と演習

標的型攻撃への対策

- Pass-the-Hash攻撃などの攻撃手法



攻撃の「シナリオ」を
進行させない

▼

資格情報の奪取を防ぐ

標的型攻撃への対策

- Windowsで攻撃に利用されるツールの例

ツール名	ツール概要	実行結果
Mimikatz	記憶された認証情報を搾取	キャッシュされているユーザーの資格情報をディスク上から取得
gsecdump	SAM/ADやログオンセッションから、ハッシュを抽出	ログオン中のユーザーの資格情報をプロセスから取得
Pwdump7	システム内のパスワードハッシュ一覧を表示	ローカルユーザーの資格情報をディスク上から取得
QuarksPwDump	ローカル・ドメインアカウントのNTLMハッシュや、キャッシュされたドメインパスワードを取得	ローカル・ドメインユーザーの資格情報をディスク上から取得

標的型攻撃への対策

- Windowsでのツールの評価

  ツールの実施結果

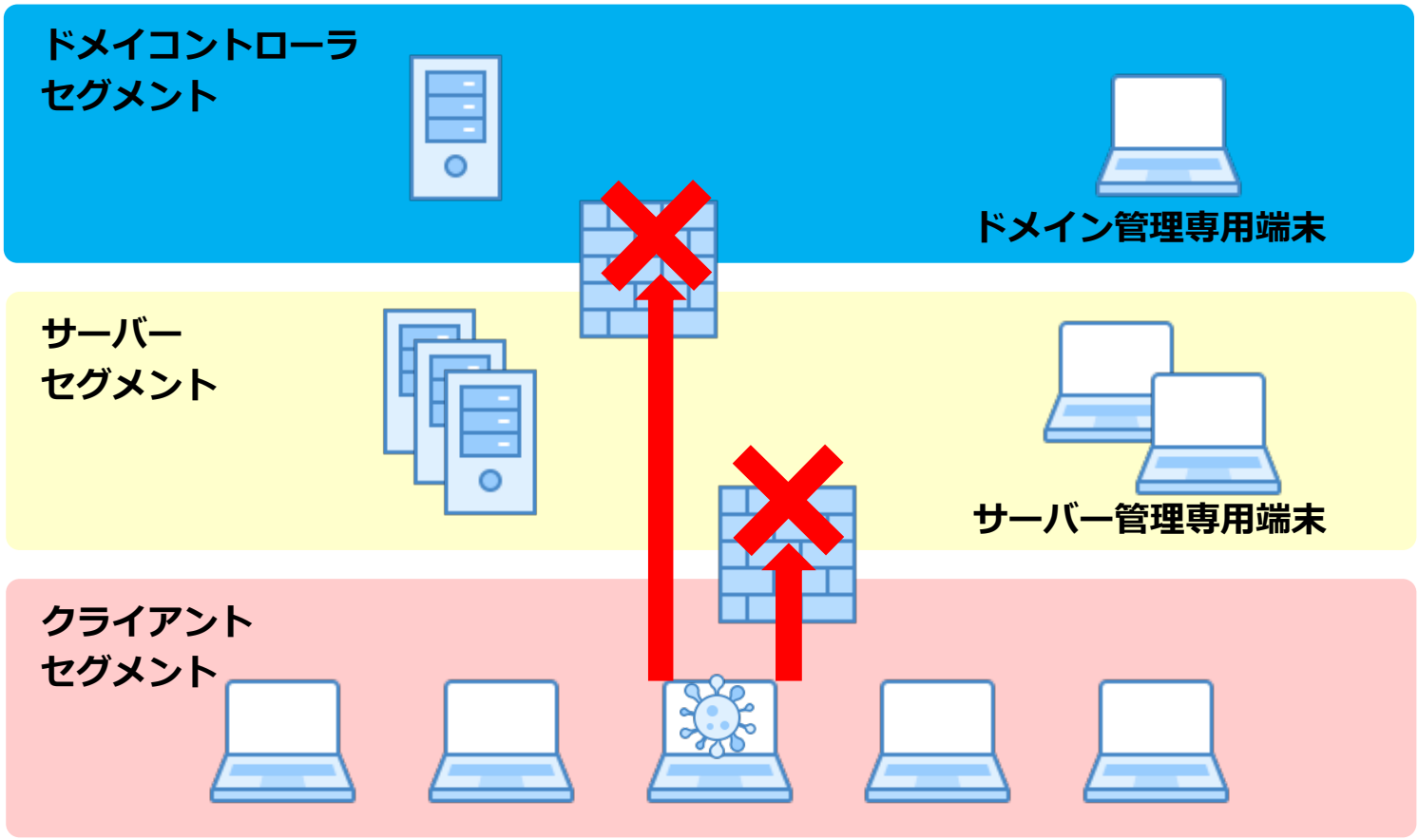
ツール名	Windows7	Windows10
Mimikatz	成功	成功
gsecdump	成功	失敗
Pwdump7	成功	失敗
QuarksPwDump	成功	失敗

出典：FFRI Windows10 セキュリティ評価支援報告書

Windows10は7に比べて格段にセキュリティレベルが向上。
しかし、それを破るための攻撃手法も継続的に開発されている。

標的型攻撃への対策

- 管理専用端末の設置



標的型攻撃への対策

- 管理専用端末の条件と必要事項

管理専用端末の設置	
適用対象	ドメインコントローラやサーバー管理に使用する端末。 (ドメイン管理者アカウントやサーバの管理者アカウントを使用する端末)
前提条件	ファイアウォールやルーターなどにより管理専用端末の通信先を制限できること。または、AppLockerなどによりプログラムの起動を制限できること。
設定手順	管理専用端末からのインターネット接続を必要最小限に制限する。 業務に不要なプログラムを起動できないように設定する。
注意事項	OSやソフトウェアの脆弱性対処のため、アップデートは必要。 更新プログラム適用に限定したインターネット接続やオフラインでの適用方法を検討する。 AppLockerは一部エディションでは使用できないので、確認する。
補足	前提条件を満たすのが難しい場合は運用ルールで制限。

管理専用端末の設置と運用

■ 運用管理セグメントの構築例

・他セグメントからアクセスできない運用管理端末専用セグメント構築
・ユーザーセグメントから運用管理セグメントへのアクセスを不可に

アクセス制御設計の例		アクセス先セグメント					
		インターネット	DMZ	サーバ	ユーザ(一般)	ユーザ(機微)	運用管理
アクセス元セグメント	インターネット		○	×	×	×	×
	DMZ	○		○	×	×	×
	サーバ	○	○		×	×	×
	ユーザ(一般)	×	×	○		×	×
	ユーザ(機微)	×	×	○	×		×
	運用管理	×	○	○	×	×	

標的型攻撃への対策

- 管理専用端末の構築（演習内容）

管理専用端末の設定内容	
認証情報の保護	制限付き保護モード(RestrictedAdmin)によるリモートデスクトップ接続の設定方法
アプリケーションの制限設定	AppLockerによるアプリケーションやプログラムの制限設定方法

認証情報の保護

- LSA Protection
- Credential Guard

	Windowsのバージョン	保護の仕組み	LSAプロセスによる資格情報管理
LSA Protection	Windows8.1～ Windows Server 2012 R2～	OS上でLSAプロセスへのアクセスを制限	する
Credential Guard	Windows 10 Enterprise	Hypervisor上でOSから機密情報を分離	しない (分離された機密側で実行)

標的型攻撃への対策

- Windows10を利用する上での考慮事項

- セキュリティレベル向上が確認された最新OS/アプリケーションの利用
- 組織(ドメイン)内のすべてのPCやサーバーに対する対応
- 脆弱性排除のためのセキュリティ更新の確実な実施
- 常に対策状況を把握し、新たに公表される脆弱性を評価して対応
- 攻撃が成功することを前提とした検知・対応の仕組みを構築

世界的な状況・法制度

世界でのサイバー攻撃や情報漏えい

- 様々な出来事や被害の判明

時期	対象	内容
2017.9	Equifax	不正アクセスにより社会保障番号を含む個人情報が流出
2017.11	Uber	2016年に不正アクセスにより個人情報が流出し、それを隠蔽していたことが発覚
2017.7	Apple	Apple社を装ったフィッシング詐欺メールが大流行
2017.10	Yahoo!	2016年の個人情報流出規模が30億人以上の全アカウントの情報が流出の可能性と判明（世界最大級）

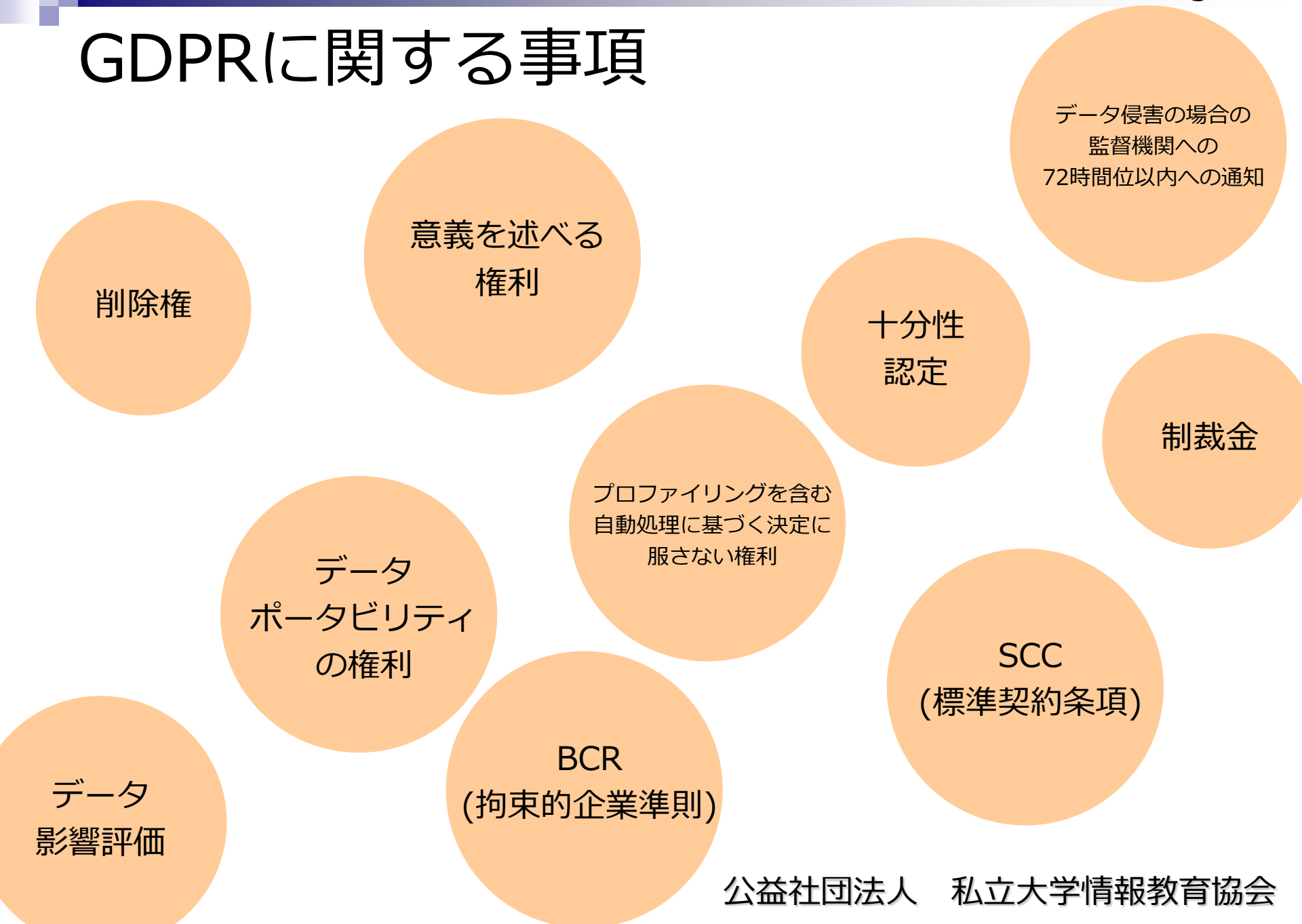
世界の法制定動向

- 米国
  2015年サイバーセキュリティ法

- EU
  NIS(Network and Information Security)指令
  GDPR(一般データ保護規則)

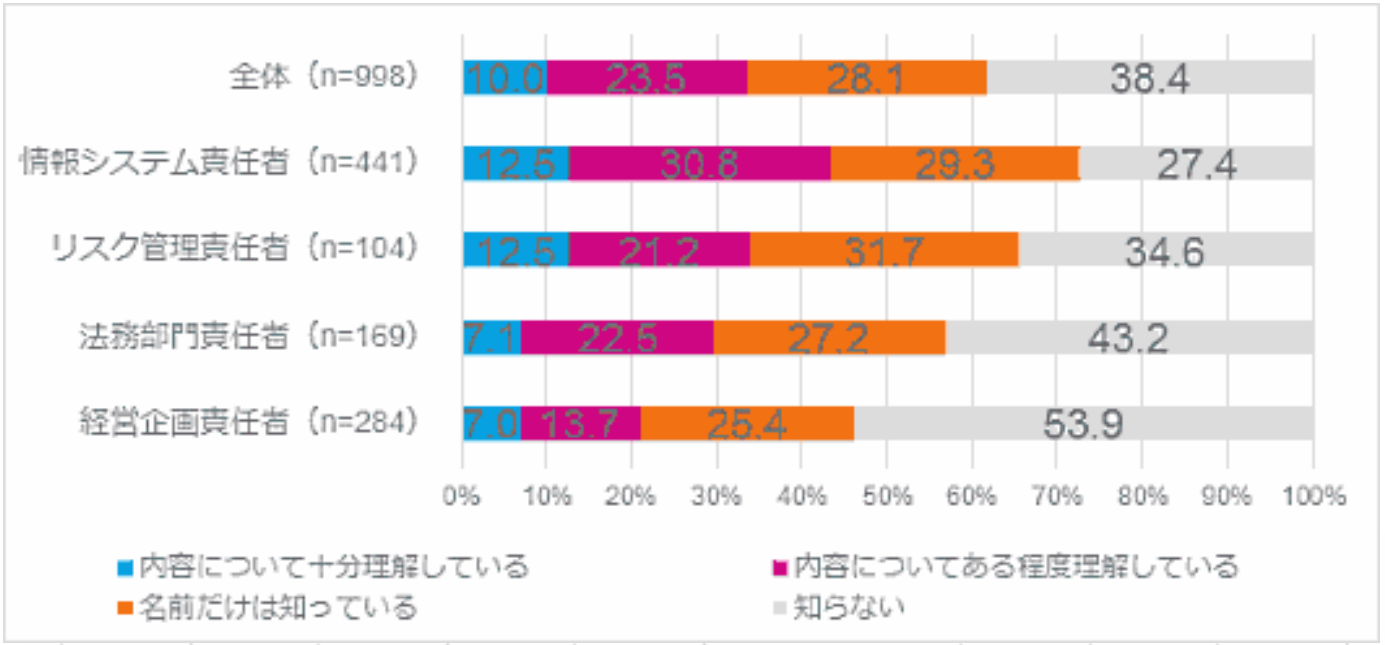
and...
EU-US プライバシーシールド

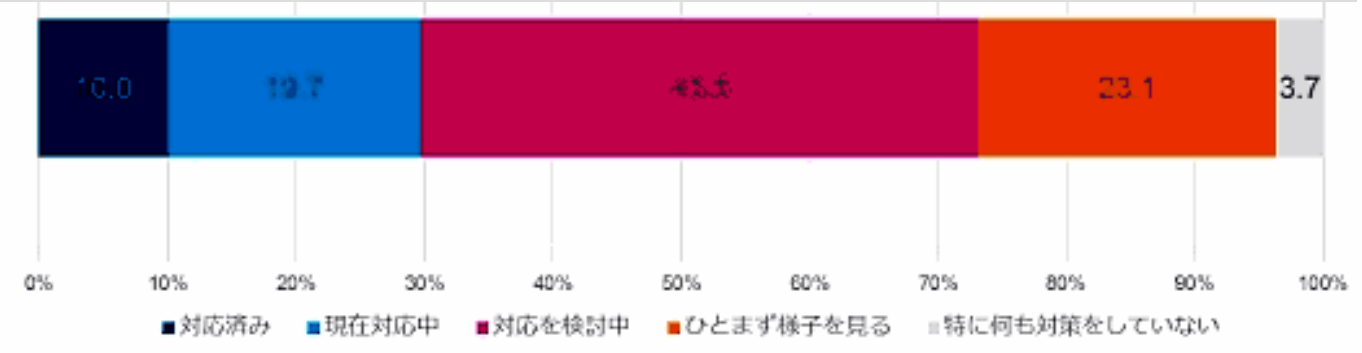
GDPRに関する事項


データ侵害の場合の
監督機関への
72時間位以内への通知
削除権
意義を述べる
権利
十分性
認定
制裁金
プロファイリングを含む
自動処理に基づく決定に
服さない権利
データ
ポータビリティ
の権利
SCC
(標準契約条項)
データ
影響評価
BCR
(拘束的企業準則)

一般データ保護規則（GDPR）2018.5

- 国内での対応状況





一般データ保護規則（GDPR）2018.5

- 違反事例？

(1-3)GDPR違反の疑いのある事例

GDPR適用を受け、特にEU居住者にサービスを提供するグローバル企業は、自社内や委託先を含め、情報の取り扱いにますます注意が必要です。

- 5/25 非営利団体noybがGoogleやFacebookなど4社を提訴しました。新しいプライバシーポリシーをユーザに強制しており、GDPRを侵害しているという主旨でした(*1-2)。
- 6/26 プリンスホテルが12万4963件の個人情報漏えいを発表しました。プリンスホテルの委託先であるFastbookingにおいて、英語、韓国語、中国語の予約システム稼働サーバが不正アクセスを受けたことが原因でした(*1-3)。

各　位

株式会社プリンスホテル

サーバーへの不正アクセスによる、当社外国語 Web サイトにてご予約いただいたお客さまの
個人情報の流出に関するお詫びとお知らせ

この度、当社の外国語 Web サイト（英語、中国語＜簡体・繁体＞、韓国語）上の予約システムについて、サーバーに対して外部から不正アクセスを受け、お客さまの個人情報が流出した事実が判明いたしました。
ご利用いただきましたお客さまをはじめ関係の皆さまには、多大なご迷惑をおかけいたしましたことを深くお詫び申しあげます。
本件については判明後、個人情報保護委員会に報告しております。
当社の外国語 Web サイトは「ファストブッキングジャパン株式会社」に運営委託しており、同社の親会社であるフランス法人「ファストブッキング社」が所有するサーバーに対して不正アクセスがございました。
なお、当社の日本語 Web サイトからご予約いただきましたお客さまの個人情報の流出はございません。
また、これまでに個人情報を悪用される等の被害の報告はございません。
詳細につきましては下記のとおりです。

GDPRへの対応

■ 優先事項とその進め方

現状把握

- 個人データの棚卸
- データ所在地の確認
- データフローの確認
- アクセス権限の確認

等

▶

対応策の計画

- 推進体制
- データ保護方針策定
- データ取扱いプロセス
- インシデント対応
- システム対応

等

▶

対応策の計画

- データ流出防止
- データの把握
- データ保護
- データ制御

等

GDPRを悪用したサイバー攻撃

- GDPR対象となる情報を盗み出した脅迫
- 対応への不安を煽るフィッシング詐欺
- GDPRを題材としたビジネスメール詐欺
- 偽のGDPR診断サイト　　等々

(1-2) GDPRに便乗したフィッシングメール攻撃

5/22 Avira社がGDPRに便乗したフィッシングメールの注意を呼びかけました(*1-1)。同メールは、GDPR対応にともなう個人情報ポリシーの変更や個人情報の取り扱いの同意を求める通知メールを装っており、Webページ上で個人情報を入力させたり、マルウェアに感染させたりします。AppleやPayPal、Airbnbといった有名企業を装った同様のフィッシングメールが複数報告されているため、ユーザは注意が必要です。安易にリンクをクリックしない、不自然な点がないか確認するなど、GDPRに関係する内容のメールは慎重に取り扱う必要があります。

従来のランサムウェア対策やフィッシング詐欺対策など加えて、
新しい対策方法を講じる必要ない。冷静な対応を。

GDPRへのシステム的対策例

- Webキャッシュ問題
- Google Analytics