

サイバーセキュリティ動向

2019年6月10日

独立行政法人情報処理推進機構
セキュリティセンター長 瓜生 和久

サイバーセキュリティ脅威の動向 —情報セキュリティ10大脅威 2019—

- 2018年に発生した社会的に影響が大きかったと考えられる情報セキュリティ事案を基に、有識者により構成される「10大脅威選考会」で審議・決定
(2019年2月公開)



<https://www.ipa.go.jp/security/vuln/10threats2019.html>

10大脅威2019

一個人向け、組織向け

昨年 順位	「個人」向け脅威	順位	「組織」向け脅威	昨年 順位
1 (注)	クレジットカード情報の不正利用	1	標的型攻撃による被害	1
1	フィッシングによる個人情報等の詐取	2	ビジネスメール詐欺による被害	3
4	不正アプリによる スマートフォン利用者への被害	3	ランサムウェアによる被害	2
New!	メール等を使った 脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した 攻撃の高まり	New!
3	ネット上の誹謗・中傷・デマ	5	内部不正による情報漏えい	8
10	偽警告によるインターネット詐欺	6	サービス妨害攻撃によるサービスの停止	9
1	インターネットバンキングの不正利用	7	インターネットサービスからの 個人情報の窃取	6
5	インターネットサービスへの不正ログイン	8	IoT機器の脆弱性の顕在化	7
2	ランサムウェアによる被害	9	脆弱性対策情報の公開に伴う悪用増加	4
9	IoT機器の不適切な管理	10	不注意による情報漏えい	12

(注) クレジットカード被害の増加とフィッシング手口の多様化に鑑み、2018年個人1位の「インターネットバンキングやクレジットカード情報等の不正利用」を本年から、①インターネットバンキングの不正利用、②クレジットカード情報の不正利用、③仮想通貨交換所を狙った攻撃、④仮想通貨採掘に加担させる手口、⑤フィッシングによる個人情報等の詐取、に分割。

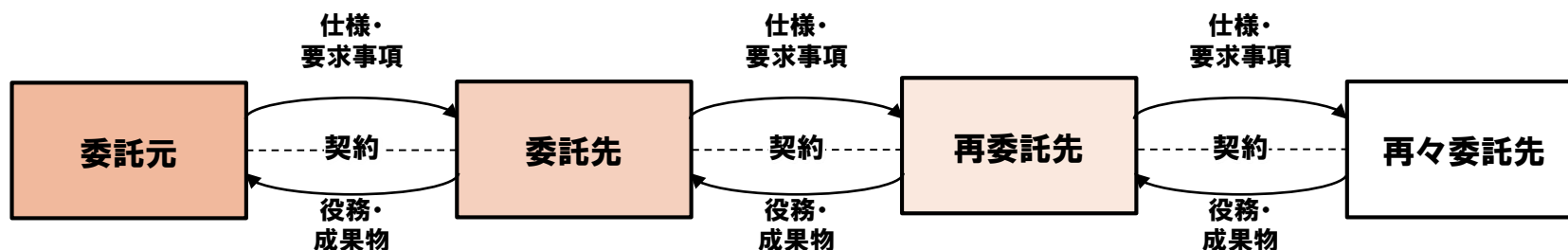
サプライチェーン攻撃について

ITサプライチェーンとは

● ITシステム・サービスの業務委託・調達の形態

- ・ システム・サービスを構成するソフトウェア、ハードウェア、サービスのライフサイクル全般(設計・開発・流通・運用・廃棄)が対象
- ・ ソフトウェアの調達＋モノの調達＋運用委託

● セキュリティ面でも企業にとって今、最も悩ましい課題のひとつ

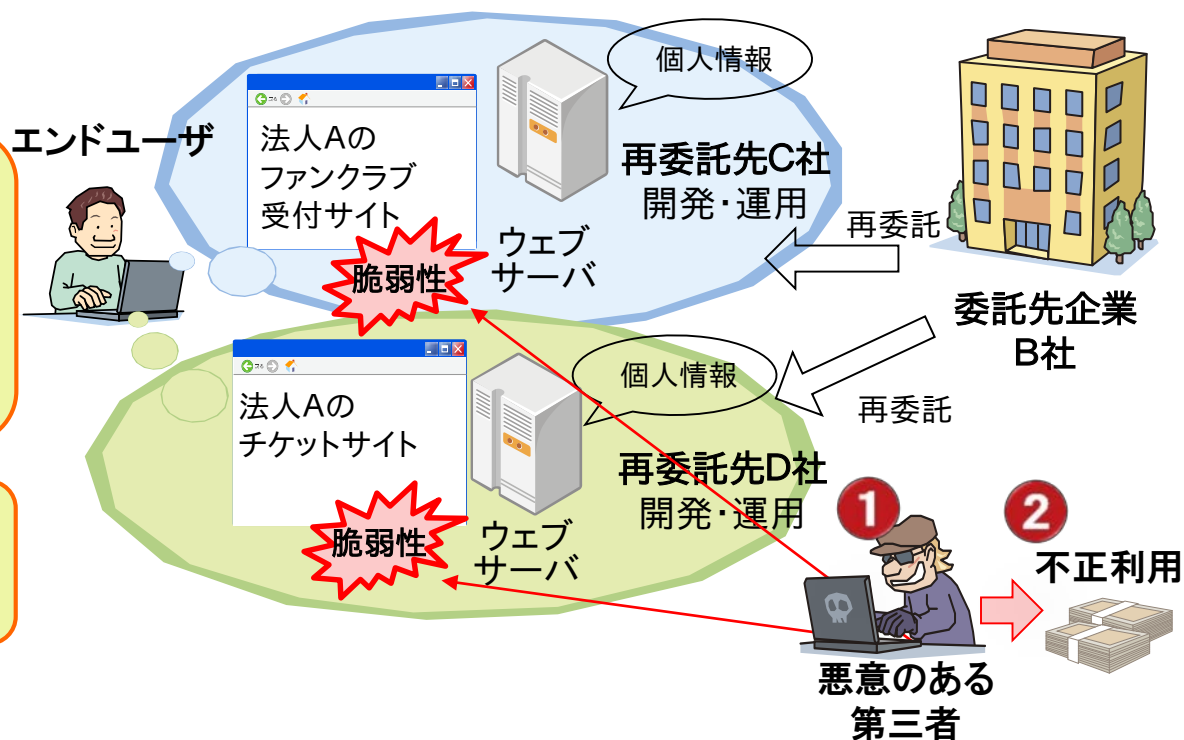


委託先へのサイバー攻撃事例

- 男子プロスポーツ法人Aの事案(業務委託先企業より公表)
- 最大約15万5千件の個人情報(クレジットカード情報約3万2千件含む)が窃取された可能性
- カードの不正利用は、379件、約880万円の被害

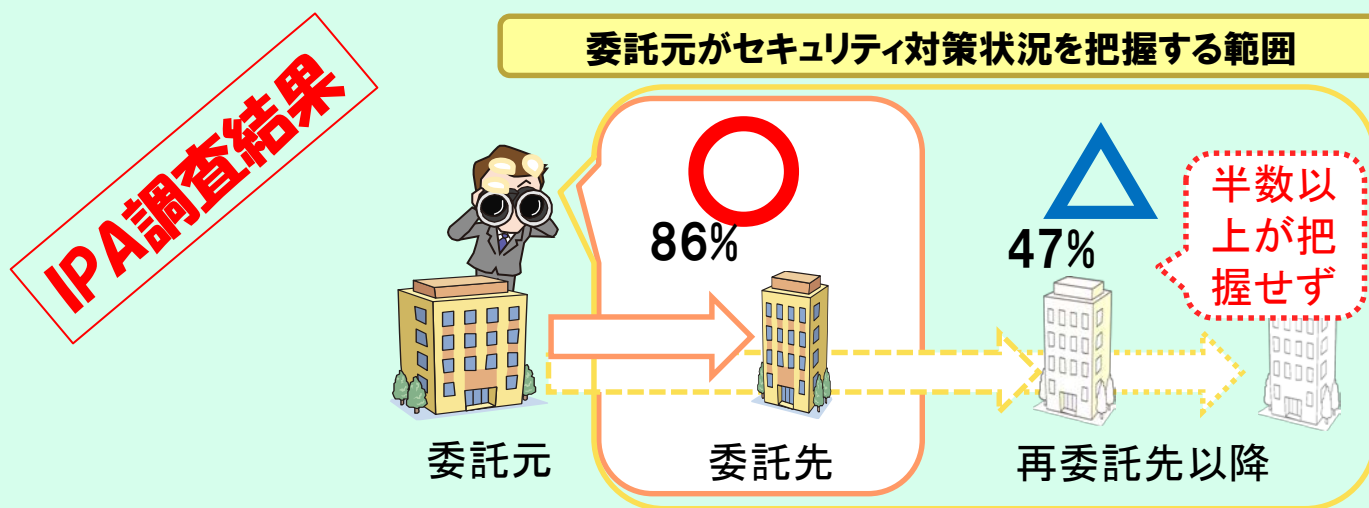
1 悪意のある第三者が公開されたApache Struts2の脆弱性を突いて、法人AのWebサーバおよびデータベースに不正アクセス、個人情報を窃取

2 窃取されたクレジットカード情報が不正利用された



直接管理できるのは直接委託先、 再委託先以降の管理は委託先任せ

- 約**86%**の組織が、**直接の取引がある委託先の状況を把握**
- 再委託先以降の取引を有する組織のうち約**47%**の組織が**再委託先以降の状況を把握**



- サプライチェーン全体の管理状況を可視化できる企業は少数
- **管理できるのは一次委託先までで、委託先以降は各委託元が管理することが現実的**

(出典) IPA「情報セキュリティに関するサプライチェーンリスクマネジメント調査」(2017年3月)

サプライチェーンパートナーの連携が大切！



- 結局、当面大切なことは…
- 委託元と委託先との情報共有
 - ・ 何が大事なのか、どう守るかを決定
 - ・ セキュリティ対策状況をどう確認するか決定・共有
 - 契約、チェックシート、ヒアリング手法など

ご参考:

サプライチェーンセキュリティ海外動向



● セキュリティ対策を実施すること＋対策が定められた基準を満たしていることの証明を要請

サイバーセキュリティ フレームワーク

重要インフラのサイバーセキュリティを
向上させるためのフレームワーク

2014年2月初版、
2018年4月1.1発行

SP800-171

連邦政府以外(民間)のシステム・
組織において利用される、格付けさ
れないが法令または政府規則により
防御・配布管理を要求される情報
(CUI)の保護の規範

Classified
Information

機密指定情報

Unclassified
Information

一般情報

Controlled
Unclassified
Information

一般情報の中でも
保護すべき情報

欧米において強化される『サプライチェーン』サイバーセキュリティへの要求

- 米国、欧州は、サプライチェーン全体に及ぶサイバーセキュリティ対策を模索。

【米国】

- 2017年、サイバーセキュリティフレームワーク (NIST策定のガイドライン) に、『サイバーサプライチェーンリスクマネジメント』を明記へ
- 2017年末、防衛調達に参加する全ての企業に対してセキュリティ対策 (SP800-171の遵守) を義務化

【欧州】

- 2016年、エネルギー等の重要インフラ事業者に、セキュリティ対策を義務化 (NIS Directive)
- 2017年、単一サイバーセキュリティ市場を目指し、ネットワークに繋がる機器の認証フレームの導入検討を発表
- EUの顧客データを扱う企業に対するデータ処理制限等の新たな義務 (GDPR) を2018年から適用
- ドイツにおいてルーターのテクニカルガイドラインを作成中

セキュリティ要件を満たさない事業者、製品、サービスは
グローバルサプライチェーンからはじき出されるおそれ

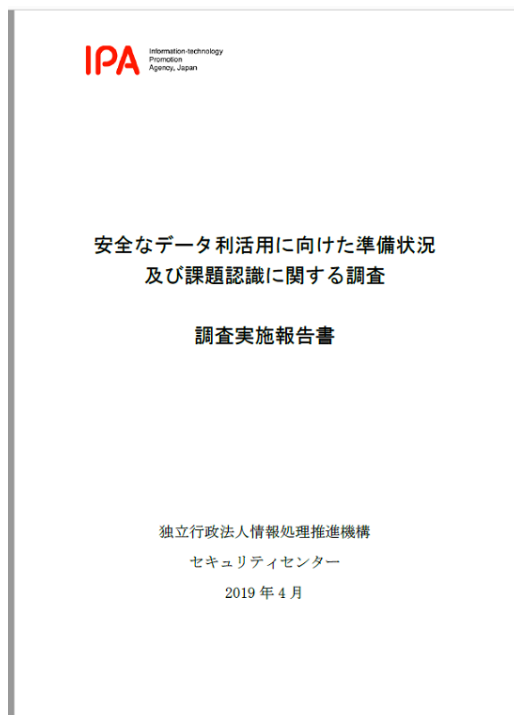
(出典) 経済産業省 産業サイバーセキュリティ研究会(第1回)
「資料5 産業分野におけるサイバーセキュリティ政策」

2018年度のIPA営業秘密関連調査： データ利活用に関する実態調査



● データ利活用の準備状況・課題認識に関する調査結果をご紹介します

https://www.ipa.go.jp/security/fy30/reports/ts_research/index.html



「安全なデータ利活用に向けた準備状況
及び課題認識に関する調査」

(東証1部、2部、マザーズ上場企業を対象：
アンケート調査 およびインタビュー調査)

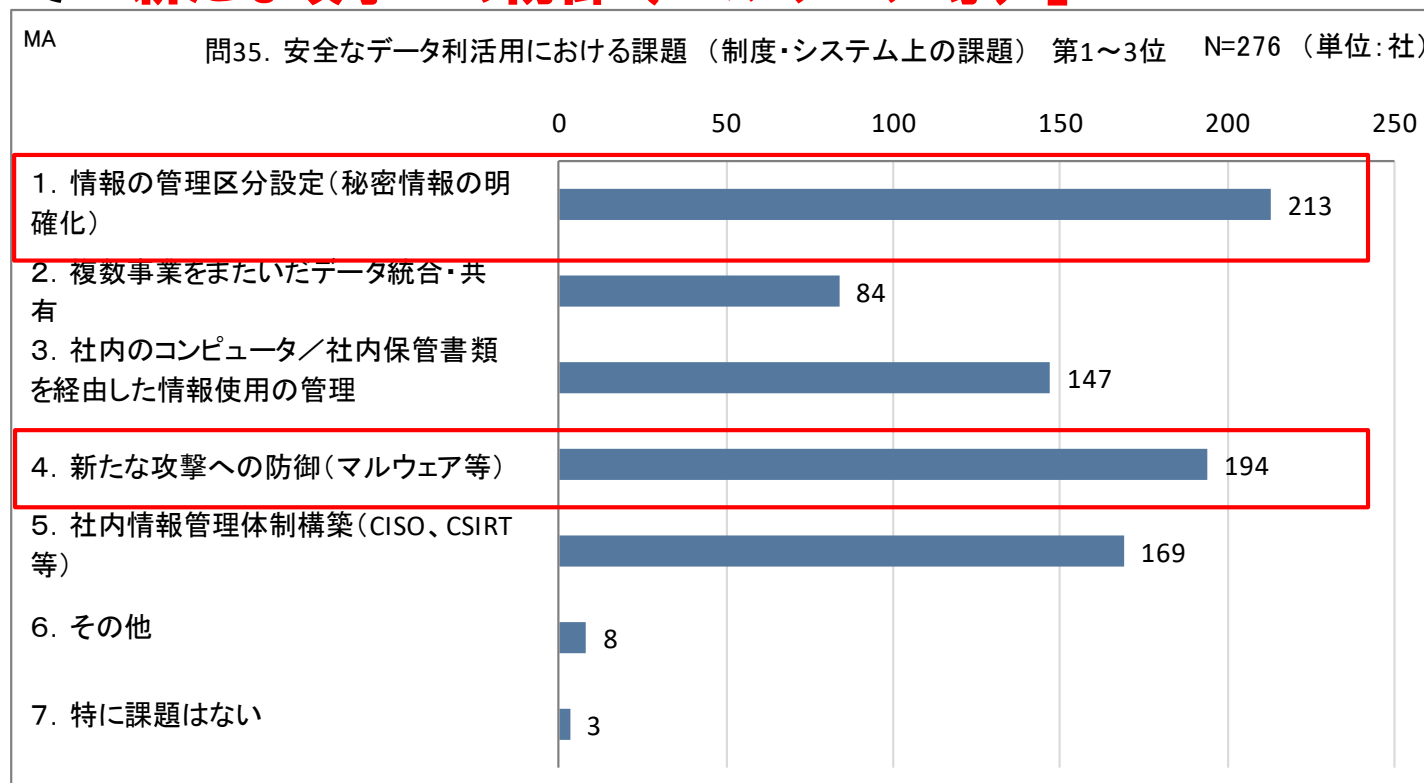
HOT TOPICS:
情報管理区分
秘密保持契約
(限定提供データ)

調査結果（抜粋）

安全なデータ利活用に関する課題・対応策①

- 「安全なデータ利活用における課題（制度・システム上の課題）」
第1～3位の合計：

**「情報の管理区分設定（秘密情報の明確化）」が最多、
次いで「新たな攻撃への防御（マルウェア等）」**



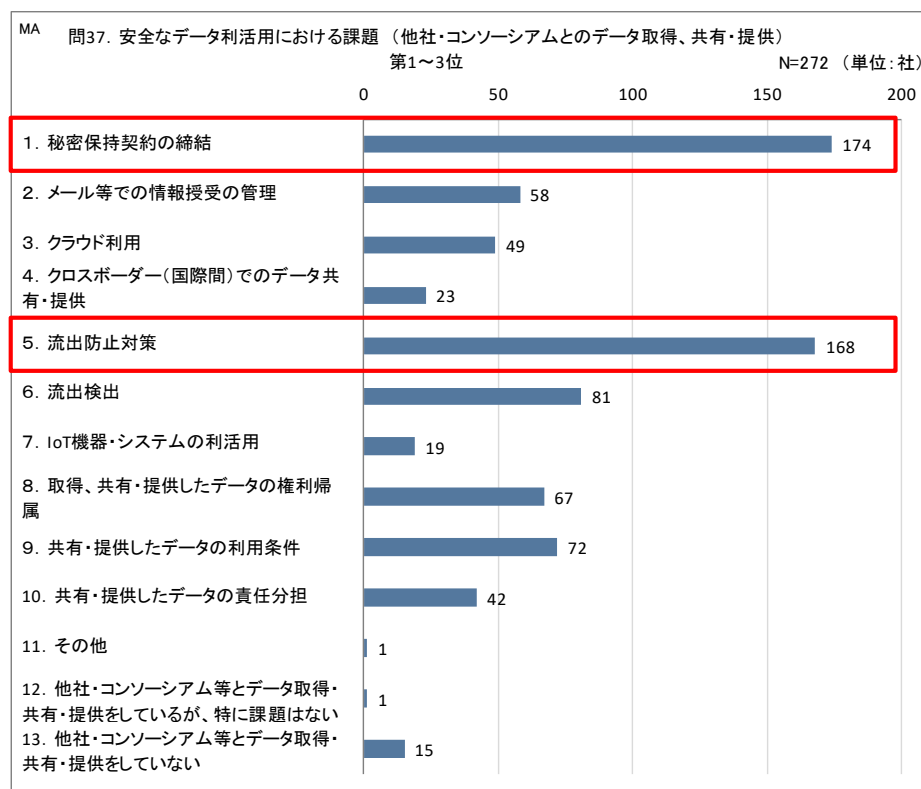
調査結果（抜粋）

安全なデータ利活用に関する課題・対応策②

- 「安全なデータ利活用における課題
（他社・コンソーシアムとのデータ取得、共有・提供）」

第1～3位の合計：

「**秘密保持契約の締結**」が最多、次いで「**流出防止対策**」



調査結果のまとめ

- データ利活用に関心のある企業は、
 - ① データ利活用の**事業収益（メリット）**
 - ② データ共有・提供先企業の**目的外利用、第3者への流失**
 - ③ 提供される**データの品質**に不安を感じている。
- データ利活用に関する事業では、**ビジネスモデル**や**成果イメージ**を具体化し、対処すべき**リスク**を見定め、**対応策**を講じることが重要である。

さいごに…

営業秘密に関する今年度の活動

データ利活用促進の要請
適正なデータ活用の必要性

調査・検討会推進

改正不正競争防止法
(限定提供データ)

「企業のデータ利活用・
保護の戦略立案のための
手引書(案)」作成
(先進事例を含む)

不正競争防止小委員会への報告
(予定)

秘密情報の保護ハンドブック
～企業価値向上に向けて～

平成28年2月

経済産業省

「秘密情報の保護ハンドブック」
(平成28年)

保護の側面を重視



IPA

独立行政法人 情報処理推進機構

Information-technology Promotion Agency, Japan