

サイバーセキュリティ動向

2018年6月13日

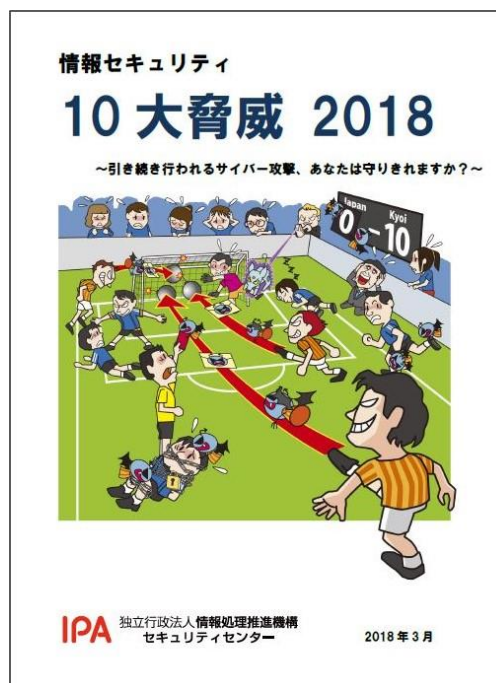
独立行政法人情報処理推進機構

理事 江口 純一

サイバーセキュリティ脅威の動向

ー情報セキュリティ10大脅威 2018ー

- 2017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における事案から、IPAが脅威候補を選出、有識者により構成される「10大脅威選考会」で審議・決定（2018年3月資料公開）



<https://www.ipa.go.jp/security/vuln/10threats2018.html>

サイバーセキュリティ脅威の動向

ー情報セキュリティ10大脅威 2018ー



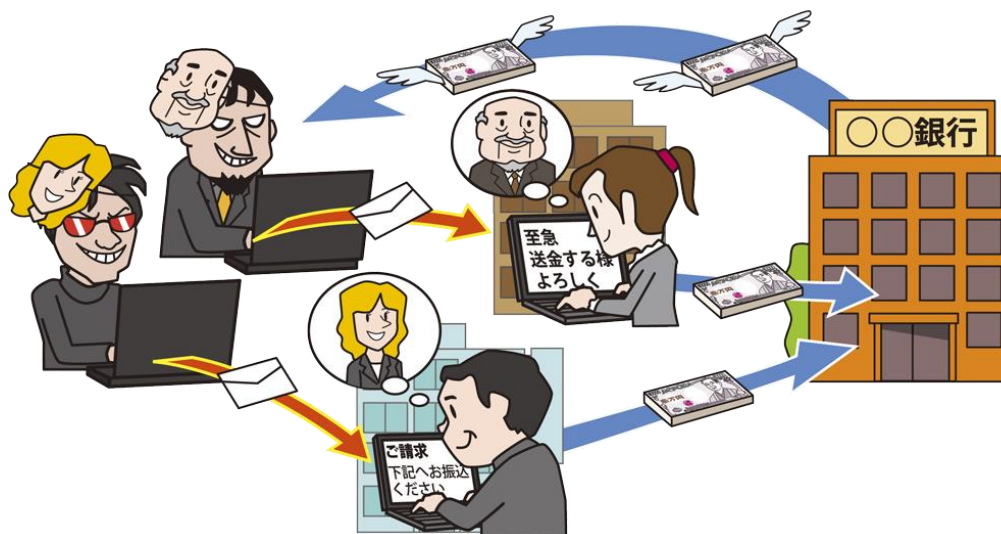
1,2位は変化なし 継続注意

昨年 順位	「個人」向け脅威	順位	「組織」向け脅威	昨年 順位
1	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	1	標的型攻撃による被害	1
2	ランサムウェアによる被害	2	ランサムウェアによる被害	2
7	ネット上の誹謗・中傷	3	New! ビジネスメール詐欺による被害	ラン ク外
3	スマートフォンやスマートフォンアプリを 狙った攻撃	4	New! 脆弱性対策情報の公開に伴う 悪用増加	ラン ク外
4	ウェブサービスへの不正ログイン	5	New! 脅威に対応するための セキュリティ人材の不足	ラン ク外
6	ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取	3
8	情報モラル欠如に伴う犯罪の低年齢化	7	IoT機器の脆弱性の顕在化	8
5	ワンクリック請求等の不当請求	8	内部不正による情報漏えい	5
10	IoT機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止	4
ラン ク外	偽警告による インターネット詐欺	10	犯罪のビジネス化 (アンダーグラウンドサービス)	9

ビジネスメール詐欺による被害

【10大脅威 組織 3位】

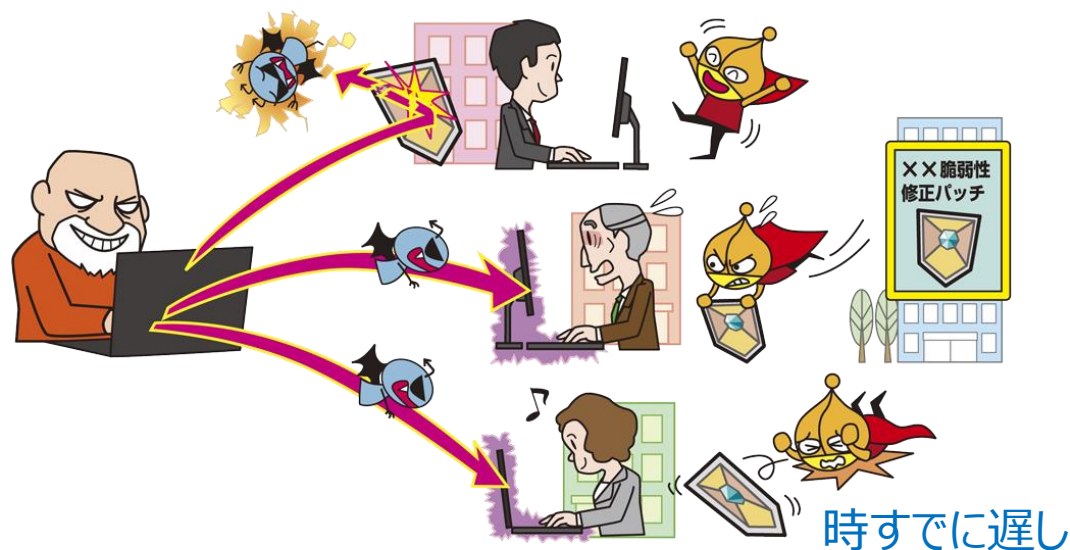
- 巧妙にメールのやりとりを偽装、企業の担当者を騙し、攻撃者の用意した口座へ送金させ詐取する手口



- 取引先との請求書の偽装
- 経営者等へのなりすまし
- 窃取メールアカウントの悪用

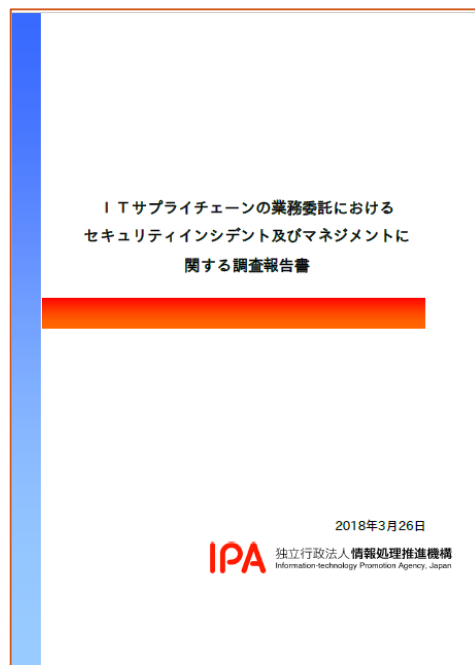
脆弱性対策情報の公開に伴う悪用増加 【10大脅威 組織 4位】

- ソフトウェアの脆弱性情報を攻撃者に悪用され、当該ソフトウェア製品を利用した対策前のシステムを狙う攻撃



- 対策適用前の脆弱性を悪用
- 脆弱性対策情報が公開される前の脆弱性を悪用
(ゼロデイ攻撃)

- ITサプライチェーン（業務委託等）におけるセキュリティリスクに関する調査結果ご紹介（2017年度実施）



サプライチェーンからの
営業秘密漏えいリスクも！

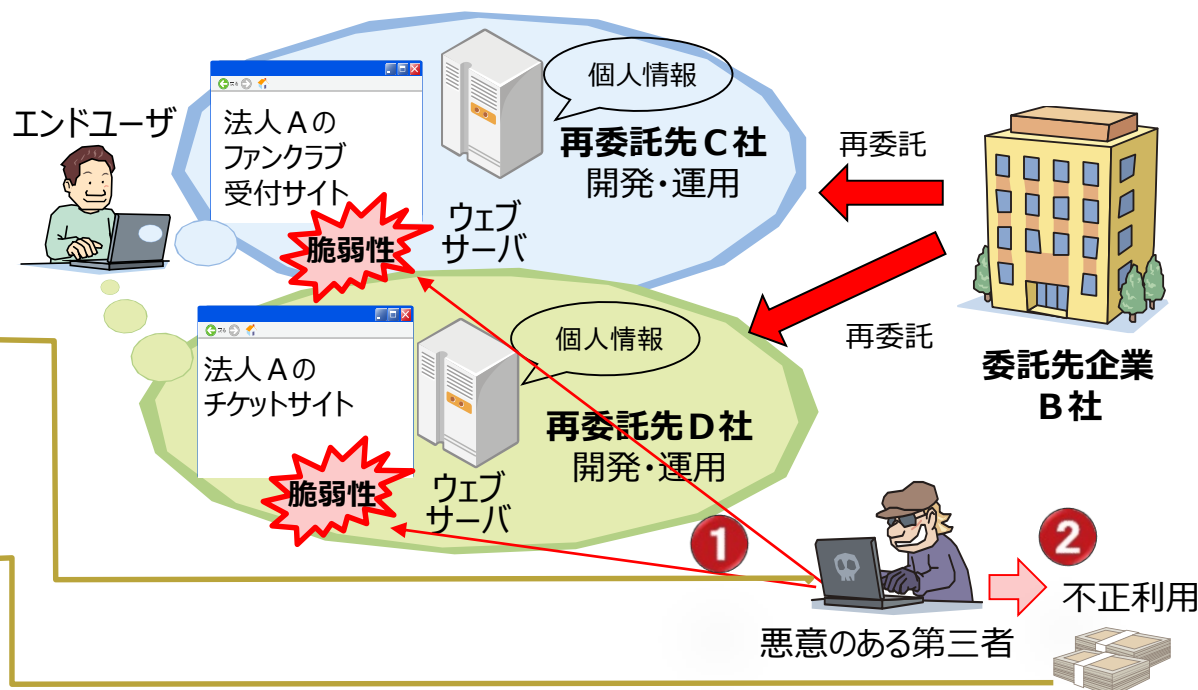
<https://www.ipa.go.jp/about/press/20180326.html>

国内インシデント事例：サイバー攻撃

- 男子プロスポーツ法人 A の事案（2017年4月25日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（または閲覧）された可能性
- カードの不正利用は、379件、約880万円の被害報告（2017年5月時点）

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

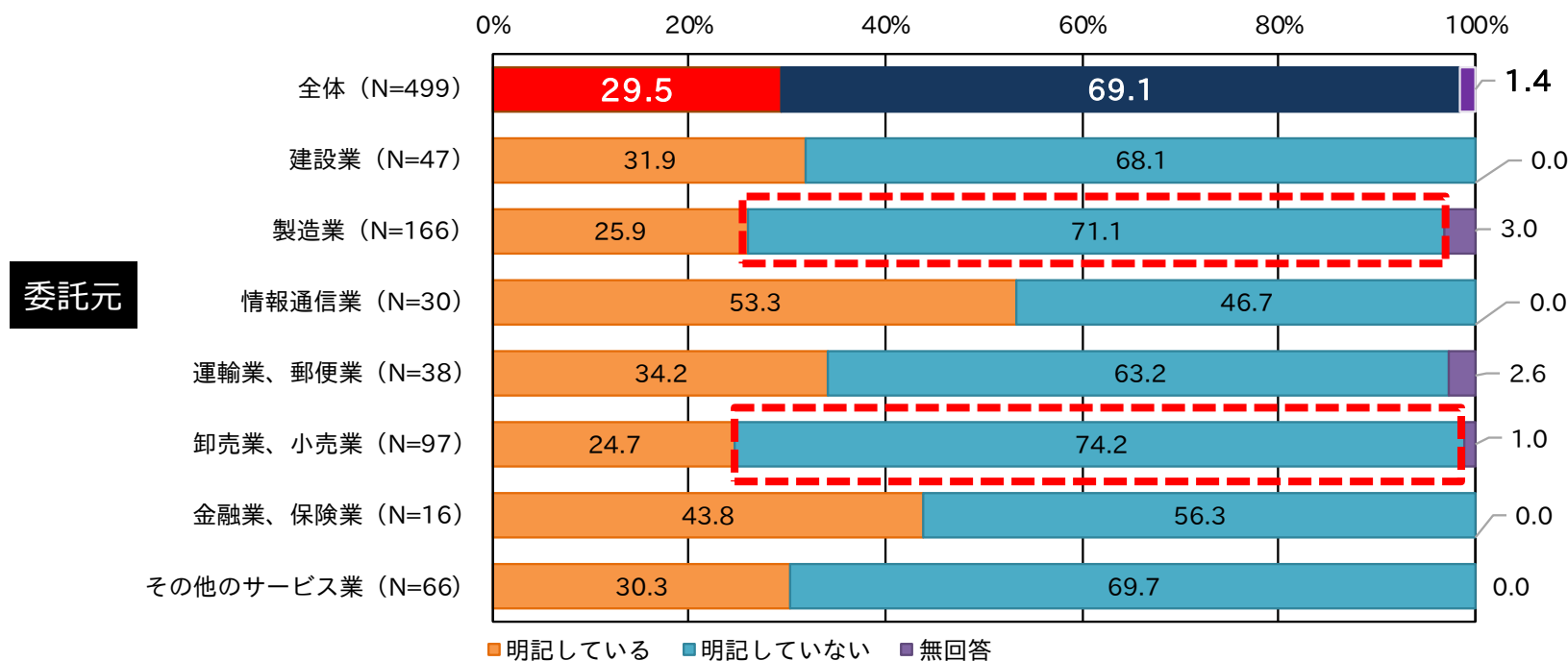
② 窃取されたクレジットカード情報が不正利用された



委託元の情報セキュリティに関する要件は仕様書等で委託先に明示できていない

- 情報セキュリティ対策を仕様書等に明記していないのは69.1%
製造業は71.1%、卸売業、小売業は74.2%と顕著
- 業種により相当の差

委託先が実施すべき具体的な情報セキュリティ対策の仕様書等での明記（全体／業種別）

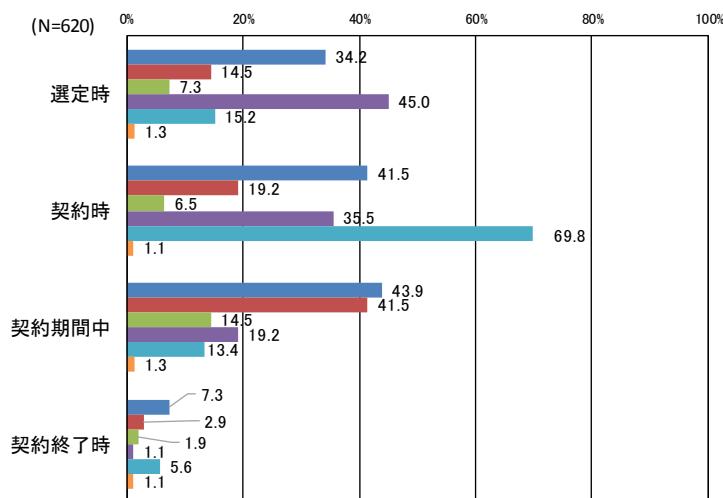


委託先のセキュリティ対策実施状況 報告は自己申告が多い

- 委託元の要求に従い様々な方法・各段階で情報セキュリティ対策の実施状況を報告
 - ・ **チェックリスト**（委託先の**自己申告**）がどの段階でも多い
 - ・ 各種認証・制度**取得証明書**は選定時、**誓約書**は契約時、**実地監査**は期間中が多い
- 複数の委託元からの確認あり／対応部門の負担大

委託先の状況

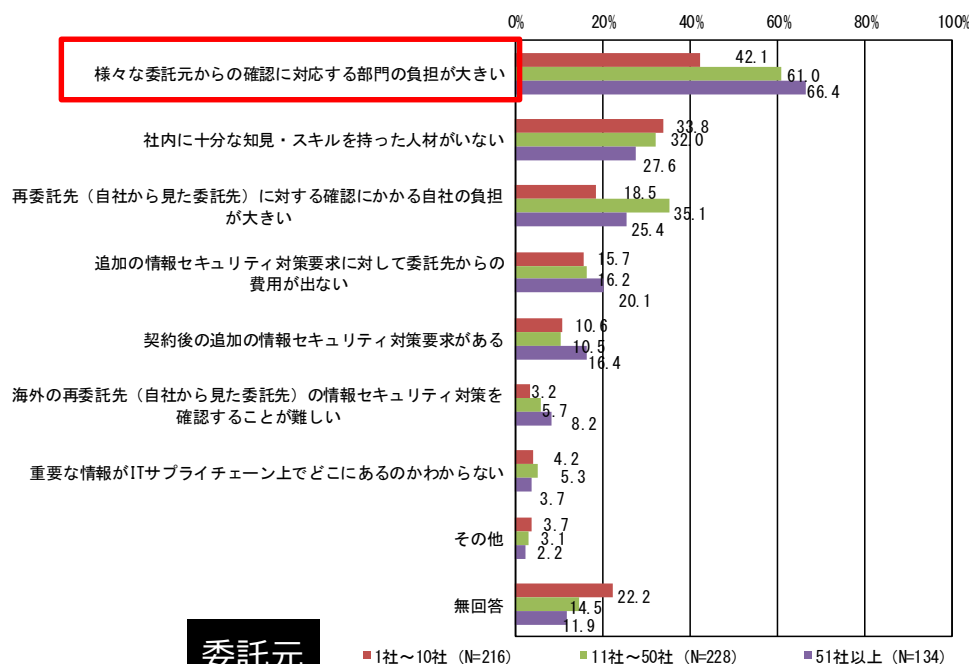
委託元からの情報セキュリティ対策の実施状況の確認方法・タイミング



- チェックリストなど(自社のセルフチェック・内部監査)
- 実地調査(委託元による自社の監査)
- 外部監査(外部監査法人等による自社の監査)
- 各種認証・制度(ISMS、Pマーク等)の取得証明書
- 誓約書
- その他

確認方法

委託元による情報セキュリティ対策の確認等における課題
(委託先、直接取引を行う委託元の社数別)

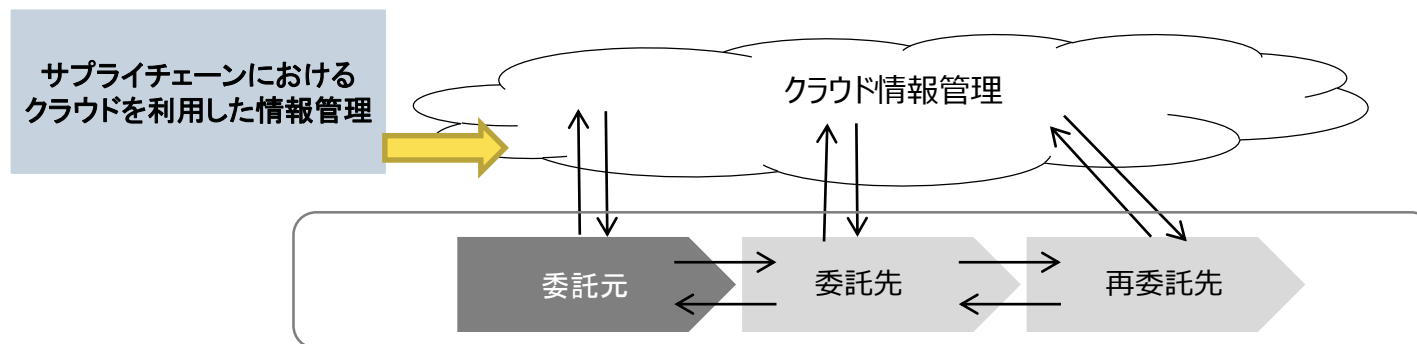


委託元

■ 1社～10社 (N=216) ■ 11～50社 (N=228) ■ 51社以上 (N=134)

調査事例： クラウドを活用したサプライチェーン横断的情報管理

- 「第四次産業革命を踏まえた秘密情報の管理と利活用におけるリスクと対策に関する調査」
(2017年度実施) でもクラウド関連リスクを調査



サプライチェーン横断的なクラウドの利用はすでに始まっている（ヒアリング調査結果）

得られた注意点は

- ・クラウドに格納するデータを整理し、規定すること
- ・パブリッククラウドのベンダー選定・申請の厳格化
- ・クラウドへ転送するデータの監視・フィルタリング技術の導入 等



独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan