資　料　編

目　　次

- サイバー事案の被害の潜在化防止に向けた検討会　委員名簿 …… 1
- サイバー事案の被害の潜在化防止に向けた検討会　開催状況 …… 2
- 個人情報保護委員会における漏えい等事案への対応 …… 3
- 医療分野におけるサイバーセキュリティ被害の実態とセキュリティ上の課題 …… 20
- クレジットカード決済におけるサイバーセキュリティ事案の犯罪抑止に向けて …… 24

サイバー事案の被害の潜在化防止に向けた検討会　委員名簿

○ 委　員

新 井　　悠	（株）ＮＴＴデータ　システム技術本部 サイバーセキュリティ技術部 エグゼクティブ・セキュリティ・アナリスト
荒 木　粧 子	（株）ソリトンシステムズ　ＩＴセキュリティ事業部 エバンジェリスト
沢 田 登 志 子	（一社）ＥＣネットワーク　理事
篠 田　佳 奈	（株）ＢＬＵＥ　代表取締役
島 根　　悟	（一財）日本サイバー犯罪対策センター　業務執行理事
蔦　　大 輔	森・濱田松本法律事務所　弁護士
林　　憲 明	フィッシング対策協議会　運営委員
藤 本　正 代	情報セキュリティ大学院大学　教授
星　周 一 郎	東京都立大学　法学部　教授

（敬称略・５０音順）

サイバー事案の被害の潜在化防止に向けた検討会　開催状況

第１回検討会　令和４年12月12日（月）

第２回検討会　令和５年１月18日（水）

第３回検討会　令和５年３月13日（月）

サイバー事案の被害の潜在化防止に向けた検討会
～個人情報保護委員会における漏えい等事案への対応～

個人情報保護委員会
Personal Information Protection Commission

目次

Ⅰ　改正個人情報保護法

Ⅱ　委員会の監視・監督権限

Ⅲ　安全管理措置

Ⅳ　漏えい等報告件数

Ⅴ　不正アクセスの具体事例

Ⅵ　警察庁との連携検討において期待すること

Ⅰ　改正個人情報保護法

Ⅰ.改正個人情報保護法

１．令和２年改正法と令和３年改正法

令和2年改正法
令和4年4月全面施行

いわゆる３年ごと見直し規定に基づく改正

個人の権利利益の保護と活用の強化、越境データの流通増大に伴う新たなリスクへの対応、ＡＩ・ビッグデータ時代への対応等

- ✓ 利用停止・消去等の拡充、漏えい等の報告・本人通知
- ✓ 不適正利用の禁止
- ✓ 仮名加工情報の創設、個人関連情報の第三者提供制限
- ✓ 越境移転に係る情報提供の充実　等

令和3年改正法
令和４年４月一部施行
（地方部分は令和５年４月施行）

デジタル社会形成整備法に基づく改正

官民を通じた個人情報保護制度の見直し（官民一元化）

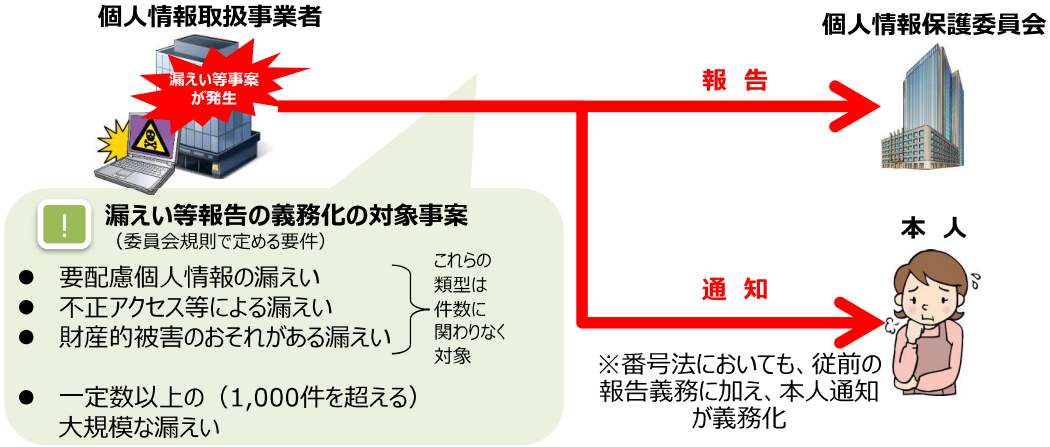
- ✓ 官民通じた個人情報の保護と活用の強化
- ✓ 医療分野・学術分野における規制の統一
- ✓ 学術研究に係る適用除外規定の見直し　等

Ⅰ.改正個人情報保護法

2．漏えい等報告の義務化

●漏えい等が発生し、個人の権利利益を害するおそれが大きい場合に、**委員会への報告及び本人への通知を義務化**する。

改正前	改正後
個人情報保護委員会に報告することは**努力義務**であり、本人通知することは**望ましい**（委員会告示）	漏えい等が発生し、個人の権利利益を害するおそれが大きい場合に、**個人情報保護委員会への報告及び本人への通知を義務化**する（§26）



4

Ⅰ.改正個人情報保護法

3．不適正な方法による利用の禁止

● **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

改正前	改正後
個人情報取扱事業者は個人情報を**適正に取得すべき**ことを法定（§20）	「適正な取得」義務に加えて、**「不適正な利用」を禁止** ※具体的には、**違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない**旨を法定（§19）

？ 「違法又は不当な行為を助長する等の不適正な方法」とは？

例えば、下記のような、**相当程度悪質なケース**が想定されます。

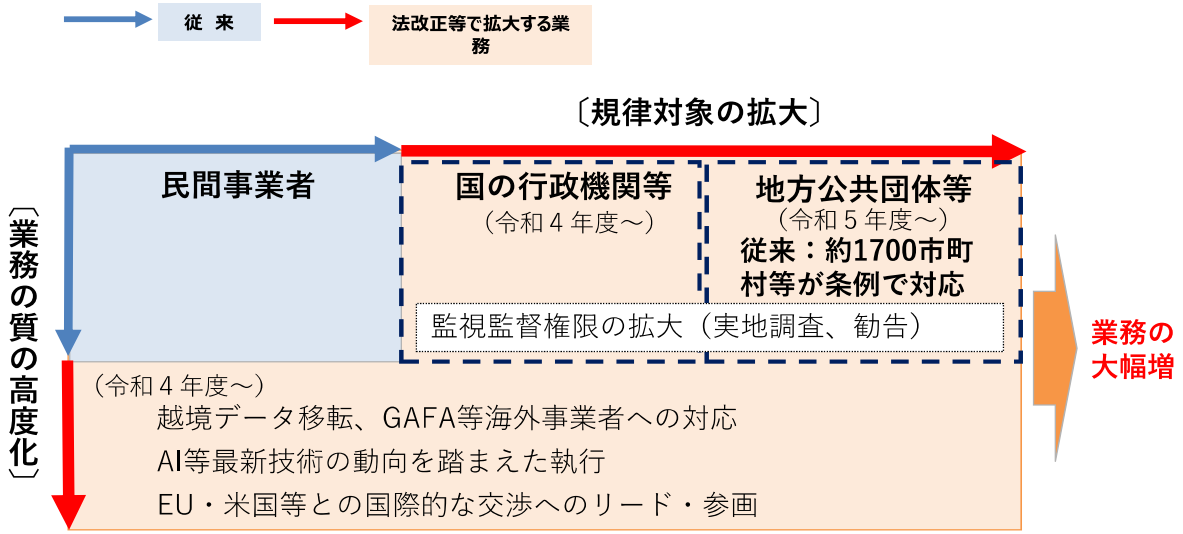
① 違法行為を営む第三者に**個人情報を提供すること。**

② 裁判所による公告等により散在的に公開されている個人情報について、差別が誘発されるおそれがあることが十分に予見できるにもかかわらず、それを**集約してデータベース化し、インターネット上で公開すること**。

5

Ⅰ.改正個人情報保護法

４．個人情報の取扱いに関する一元的な監視・監督



- 国の行政機関等については、令和４年度より計画的な実地調査、漏えい等報告の受付及び施行状況調査の実施などの監視監督活動を行っている。
- 地方公共団体等に対する監視監督活動については検討中。

6

（参考） 官民を通じた個人情報保護制度の見直し（官民一元化）①

① 個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の**3本の法律を1本の法律に統合**するとともに、**地方公共団体の個人情報保護制度**についても**統合後の法律において全国的な共通ルールを規定**し、**全体の所管を個人情報保護委員会に一元化。**

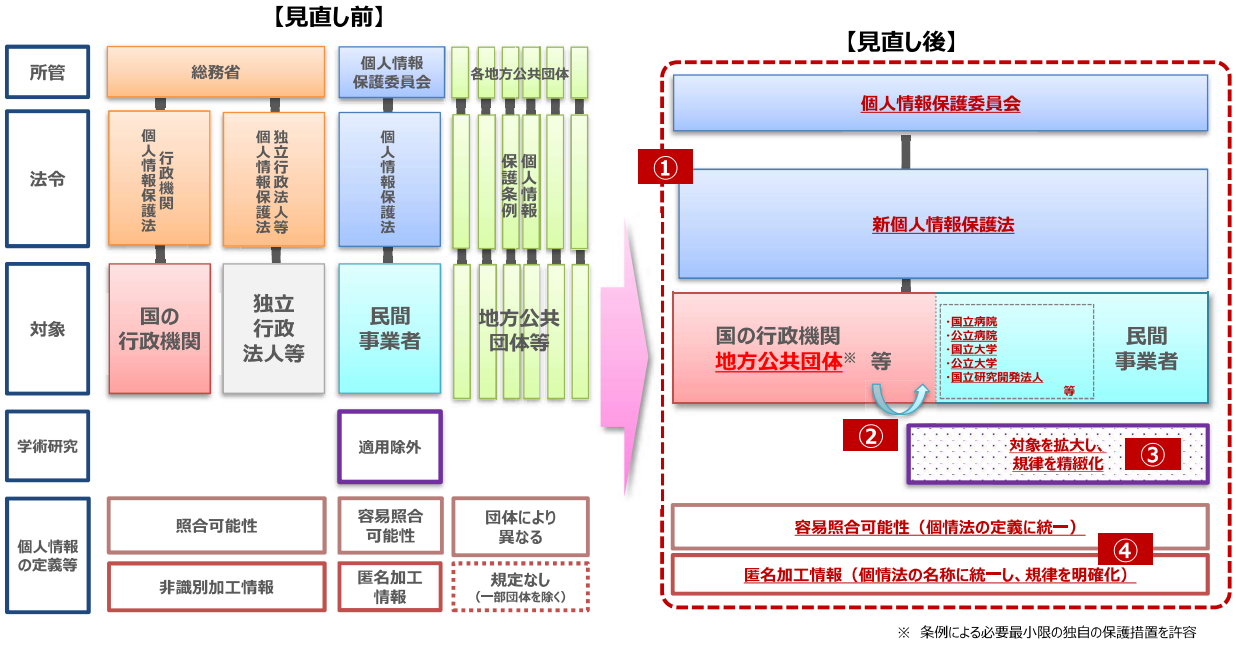
② 医療分野・学術分野の規制を統一するため、**国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用。**

③ 学術研究分野を含めたGDPRの十分性認定への対応を目指し、**学術研究に係る適用除外規定**について、一律の適用除外ではなく、**義務ごとの例外規定として精緻化。**

④ **個人情報の定義等を国・民間・地方で統一**するとともに、行政機関等での**匿名加工情報の取扱いに関する規律を明確化。**

7

（参考）　官民を通じた個人情報保護制度の見直し（官民一元化）　②



8

Ⅱ　委員会の監視・監督権限

9

Ⅱ．委員会の監視・監督権限

（１）個人情報保護法※1に基づく権限①

根拠条文

個人情報保護委員会の監視・監督権限

・個人情報取扱事業者※2のその取り扱う個人データ※3の漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則※4で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより当該事態が生じた旨を個人情報保護委員会に報告（法第26条①）
・　〃　等への報告徴収・立入検査（法第143条）
・　〃　等への指導及び助言（法第144条）
・　〃　等への勧告及び命令（法第145条）
・行政機関の長等は、保有個人情報の漏えい、滅失、毀損その他の保有個人情報の安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則※5で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告（法第68条①）
・　〃　への実地調査（法第153条）
・　〃　への指導及び助言（法第154条）
・　〃　への勧告（法第155条）

※1「個人情報保護法」…個人情報の保護に関する法律（平成15年法律第57号）
※2「個人情報取扱事業者」…個人情報データベース等（個人情報を含む情報の集合物であって、特定の個人情報を検索できるように体系的に構成したの）を事業の用に供している者（国の機関等を除く）
※3「個人データ」…個人情報データベース等を構成する個人情報
※4「規則」…内容詳細はP11参照
※5「規則」…内容詳細はP12参照

10

Ⅱ．委員会の監視・監督権限

（１）個人情報保護法に基づく権限②

根拠条文

法第26条関係（民間部門）規則※第7条…個人の権利利益を害するおそれが大きいもの

第1号：要配慮個人情報が含まれる個人データの漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある事態

第2号：不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

第3号：不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

第4号：個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

※「規則」…個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号）

11

Ⅱ．委員会の監視・監督権限

（１）個人情報保護法に基づく権限③

根拠条文

法第68条関係（公的部門）規則※1第43条…個人の権利利益を害するおそれが大きいもの

第1号：要配慮個人情報が含まれる保有個人情報※2の漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある事態

第2号：不正に利用されることにより財産的被害が生じるおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態

第3号：不正の目的をもって行われたおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態

第4号：保有個人情報に係る本人の数が百人を超える漏えい等が発生し、又は発生したおそれがある事態

※1「規則」…個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号）
※2「保有個人情報」…行政機関等の職員（独立行政法人等にあっては、その役員を含む。）が職務上作成し、又は取得した個人情報であって、当該行政機関等の職員が組織的に利用するものとして、当該行政機関等が保有しているもの

12

Ⅱ．委員会の監視・監督権限

（２）番号法※１に基づく権限①

根拠条文

個人情報保護委員会の監視・監督権限

・行政機関等に対する定期的な特定個人情報の取り扱い状況についての検査（法第29条の3①）

・地方公共団体等を対象とした定期的な報告受付(法第29条の３②)

・個人番号利用事務等実施者は、特定個人情報ファイルに記録された特定個人情報の漏えい、滅失、毀損その他の特定個人情報の安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則※2で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を委員会に報告(法第29条の４)

・　〃　に対する必要な指導・助言(法第33条)

・法令違反行為者に対する是正勧告及び命令(法第34条)

・特定個人情報を取り扱う者等に対する必要な報告徴収・検査(法第35条)

※１「番号法」…行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）
※2「規則」…内容詳細はP14-15参照

13

Ⅱ．委員会の監視・監督権限

（２）番号法に基づく権限②

根拠条文

法第29条関係:規則※1第2条…個人の権利利益を害するおそれが大きいもの＜1/2＞

第1号：次に掲げる特定個人情報※2の漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある事態

イ 情報提供ネットワークシステム及びこれに接続された電子計算機に記録された特定個人情報

ロ 個人番号利用事務実施者が個人番号利用事務を処理するために使用する情報システムにおいて管理される特定個人情報

ハ 行政機関、地方公共団体、独立行政法人等及び地方独立行政法人が個人番号関係事務を処理するために使用する情報システム並びに行政機関、地方公共団体、独立行政法人等及び地方独立行政法人から個人番号関係事務の全部又は一部の委託を受けた者が当該個人番号関係事務を処理するために使用する情報システムにおいて管理される特定個人情報

※1「規則」…行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の4第1項及び第2項に基づく特定個人情報の漏えい等に関する報告等に関する規則（平成27年特定個人情報保護委員会規則第5号）
※2「特定個人情報」…個人番号をその内容に含む個人情報

14

Ⅱ．委員会の監視・監督権限

根拠条文

法第29条関係:規則第2条…個人の権利利益を害するおそれが大きいもの＜2/2＞

第2号：次に掲げる事態

イ 不正の目的をもって行われたおそれがある特定個人情報の漏えい等が発生し、又は発生したおそれがある事態

ロ 不正の目的をもって、特定個人情報が利用され、又は利用されたおそれがある事態

ハ 不正の目的をもって、特定個人情報が提供され、又は提供されたおそれがある事態

第3号：個人番号利用事務実施者又は個人番号関係事務実施者の保有する特定個人情報ファイルに記録された特定個人情報が電磁的方法により不特定多数の者に閲覧され、又は閲覧されるおそれがある事態

第4号：次に掲げる特定個人情報に係る本人の数が百人を超える事態

イ 漏えい等が発生し、又は発生したおそれがある特定個人情報

ロ 番号法第９条の規定に反して利用され、又は利用されたおそれがある個人番号を含む特定個人情報

ハ 番号法第19条の規定に反して提供され、又は提供されたおそれがある特定個人情報

15

Ⅲ　安全管理措置

16

Ⅲ．安全管理措置

（１）個人情報取扱事業者の安全管理措置

根拠条文　**個人情報保護法第23条**

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない

（２）行政機関等の安全管理措置

根拠条文　**個人情報保護法第66条①**

行政機関の長等は、保有個人情報の漏えい、滅失又は毀損の防止その他の保有個人情報の安全管理のために必要かつ適切な措置を講じなければならない

（３）個人番号利用事務実施者等の安全管理措置

根拠条文　**番号法第12条**

個人番号利用事務実施者及び個人番号関係事務実施者は、個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない

17

Ⅲ．安全管理措置

組織的安全管理措置

- 漏えい等事案が発生した場合の組織体制の整備
- アクセス権限の定期的な棚卸
- 委託先の管理
  －契約内容の確認･見直し
  －定期的な監査　など

物理的安全管理措置

- 機器･電子媒体等の管理体制の整備
- 個人データを取り扱う区域の管理
- 盗難防止のための適切な管理

外的環境の把握

- 外国において個人データを取り扱う場合、当該外国における個人情報の保護に関する制度を把握

人的安全管理措置

- セキュリティに関する定期的な研修や訓練の実施
  －標的型攻撃メール等を活用した訓練　など
- 事業者内での注意喚起や事例の共有

技術的安全管理措置

- 外部からの不正アクセスを防ぐセキュリティ上の体制整備
- 多要素認証の導入
- システム上の対策
  －セキュリティパッチの適用
  －監視システムの強化　など

18

Ⅳ　漏えい等報告件数

19

Ⅳ．漏えい等報告件数

１．漏えい等報告の処理状況-令和4年度上半期

（１）個人情報

①処理件数

	令和4年度上半期	(参考)令和3年度(半期換算)
総計	3,703件	-
内訳　個人情報取扱事業者	3,630件	2,924件
行政機関等	73件	-

②報告対象事態※1該当分の該当要件別件数（令和4年4月以降発生事案のみ）

▽個人情報取扱事業者　　件数、（）内は比率※2

規則第7条各号該当性	令和4年度上半期
第1号(要配慮個人情報)	1,688件（52%）
第2号(財産的被害のおそれ)	1,085件（33%）
第3号(不正の目的)	400件（12%）
第4号(千人超)	142件（4%）

▽行政機関等　　件数、（）内は比率※2

規則第43条各号該当性	令和4年度上半期
第1号(要配慮個人情報)	32件（66%）
第2号(財産的被害のおそれ)	0件（0%）
第3号(不正の目的)	0件（0%）
第4号(百人超)	18件（36%）

※1「報告対象事態」…個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号）第7条又は第43条に該当する漏えい等事案（内容詳細はP11～12）

※2「比率」…報告対象事態について個人情報取扱事業者又は行政機関等から報告された全件中の比率。複数の要件に該当する事案があるため、合計は100%を超える

20

Ⅳ．漏えい等報告件数

▽漏えい等した人数-令和4年度上半期件数　（令和4年4月以降発生事案のみ）

漏えいした人数	1,000人以下	1,001～10,000人	10,001～50,000人	50,001人以上	不明
総計	3,044件	104件	24件	19件	52件
個人情報取扱事業者	2,996件	103件	24件	19件	52件
行政機関等	48件	1件	0件	0件	0件

21

Ⅳ．漏えい等報告件数

（２）特定個人情報

①処理件数

	令和4年度上半期	(参考)令和3年度上半期
総計	77件	92件
内訳　行政機関等	7件	19件
地方公共団体	35件	51件
事業者	35件	22件

②報告対象事態※1該当分の該当要件別件数（令和4年4月以降発生事案のみ）

件数、（）内は比率※2

規則第２条各号該当性	令和4年度上半期
第1号(情報提供ネットワークシステム等)	0件（0%）
第2号(不正の目的)	2件（100%）
第3号(不特定多数の者に閲覧)	0件（0%）
第4号(百人超)	2件（100%）

※1「報告対象事態」…行政手続における特定の個人を識別するための番号の利用等に関する法律第29条の4第1項及び第2項に基づく特定個人情報の漏えい等に関する報告等に関する規則（平成27年特定個人情報保護委員会規則第5号）第2条に該当する漏えい等事案（内容詳細はP14～15）

※2「比率」…報告対象事態について個人番号利用事務等実施者から報告された全件中の比率。複数の要件に該当する事案があるため、合計は100%を超える

22

Ⅳ．漏えい等報告件数

▽漏えい等した人数-令和4年度上半期件数　（令和4年4月以降発生事案のみ）

漏えいした人数	100人以下	101～500人	501～1,000人	1,001人以上	不明
総計	0件	2件	0件	0件	0件
行政機関等	0件	0件	0件	0件	0件
地方公共団体	0件	0件	0件	0件	0件
事業者	0件	2件	0件	0件	0件

23

（参考）不正アクセスの分析

発覚後の調査で、①メールに添付されたファイルを開くことでウィルスに感染、②SSL_VPN装置の脆弱性を狙った攻撃などを契機に、外部からサーバーに不正アクセスをうけ、情報が搾取されていることを確認するケースが多い

※個人情報取扱事業者からの漏えい報告のうち、第三号（不正アクセス）の発生原因における出現頻度の高い単語を大きな文字になるように可視化したもの

24

（参考）不正アクセスの分析

（主な単語の出現回数）

単語	出現回数
メール	164
アクセス	132
ファイル	131
情報	120
サーバー	113
不正	109
攻撃	103
調査	94
脆弱	86
確認	82
添付	79
外部	78
SSL_VPN	75
パスワード	75

単語	出現回数
感染	75
Emotet	73
可能	71
利用	68
原因	65
システム	61
データ	61
アカウント	54
開封	54
サイト	54
ログイン	51
メールアドレス	51
漏えい	51
社員	50

単語	出現回数
PC	47
会社	46
弊社	46
侵入	44
報告	44
ID	43
発生	43
接続	41
管理	40
不明	40
なりすまし	39
個人	39
従業	38
ネットワーク	36

25

Ⅴ　不正アクセスの具体事例

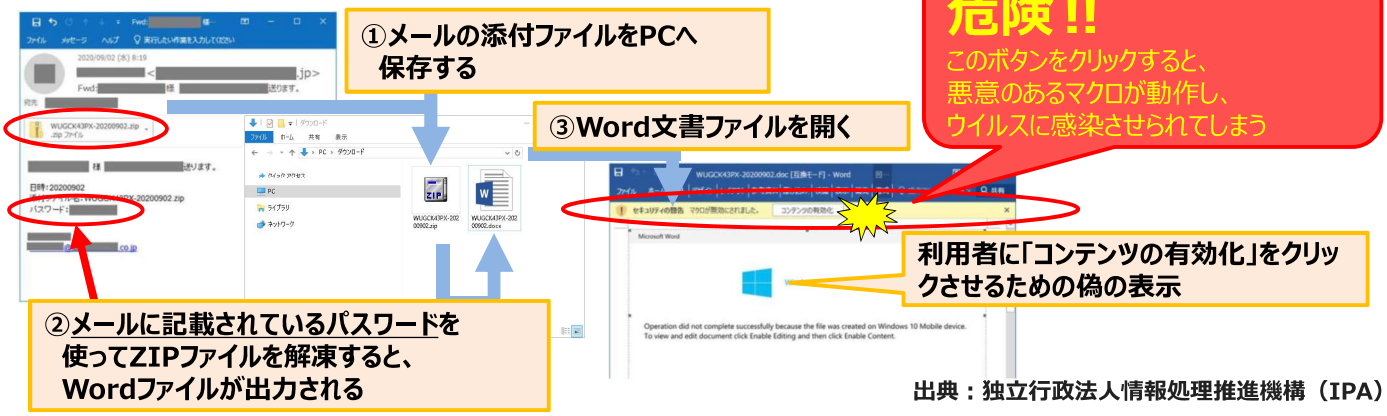
26

Ⅴ. 不正アクセスの具体事例

１.なりすましメールによるウィルス感染被害（マルウェア「Emotet」感染）

- 取引先や知人を装った受信メールに添付されたファイル、又はメール本文内の不審なURLへのアクセスによってダウンロードされるファイルを開封することによりマルウェアに感染し、メールアドレスやメール本文等の情報が漏えいする事案の報告が依然として高止まりしている。
  ※直近では攻撃側の手口が巧妙化しており、パスワード付きZIPファイルを添付し、メール配送経路上でのセキュリティ製品の検知・検疫をすり抜けるケースなども確認されている。

«パスワード付きZIPファイルからマルウェア感染までの流れ»



出典：独立行政法人情報処理推進機構（IPA）

【対策例】

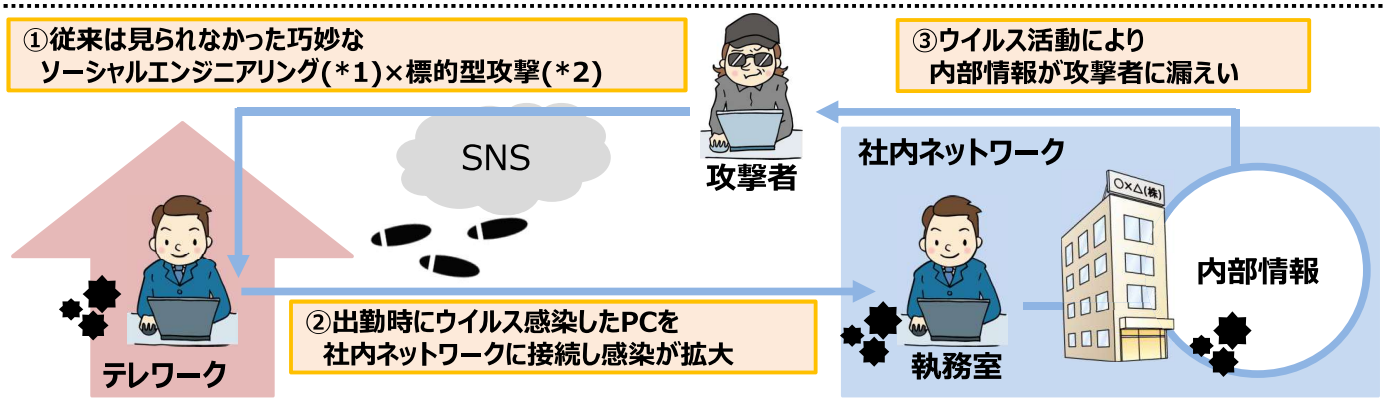
- メールアドレスのドメインや本文に不審な点がないか確認する。
- 本文を確認せずに、添付ファイルを開かない。また、不審なリンクはクリックしない。
- (攻撃側の手口が巧妙化していることから)被害に遭う可能性が一定数あると想定し、インシデント発生時の対応フローなど、事業者内で体制の整備及び周知を行う。

27

Ⅴ.不正アクセスの具体事例

2.テレワークに伴う事案（1/2）

➢ 新型コロナウイルスの影響でテレワークの利用が広がる中で、テレワーク中の社員がSNSで知り合った第三者 からウイルスが添付された電子メールを受領したことがきっかけでPCがウイルスに感染し、出勤時にそのPCを社内ネットワークに接続したことで、社内システムの情報が外部に漏えいした。



*1 本人しか知らない重要な情報を、人返心理の性質などを利用して盗み出す方法のこと。
（一見相談に乗るような手口で近づくことで信頼させ、ログインパスワードや連絡先を聞き出す等）
*2 狙いを定めた組織に対して情報の窃取や削除を目的に行われるサイバー攻撃のこと。
（その組織の従業員宛てにウイルスが添付された電子メールを送り付ける等）

【対策例】

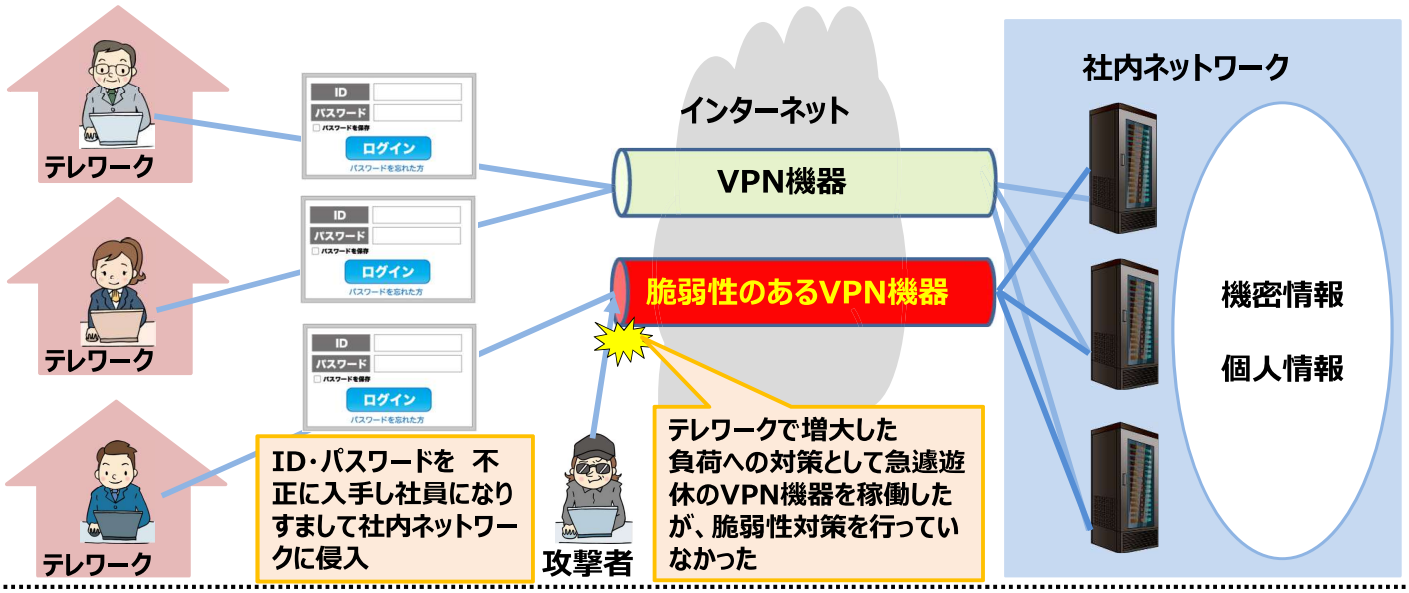
- テレワーク環境ではVPN機器へ接続しない限りインターネットを利用できない仕組みを導入することで社内と同等のセキュリティ対策を適用する。
- 少しでも不審に感じたメールに添付されているファイルやリンクは絶対にクリックしない、テレワークの場合でも一人で判断せず誰かに相談する等、従業員の方のセキュリティに対する意識を高める。
- テレワーク特有の職場とは異なる環境に則したセキュリティ確保のためのルールや相談体制を整備する。

28

Ⅴ.不正アクセスの具体事例

2.テレワークに伴う事案（2/2）

➢ 脆弱性があるVPN機器への不正アクセスにより社員の認証情報等が外部に漏えいした。



【対策例】

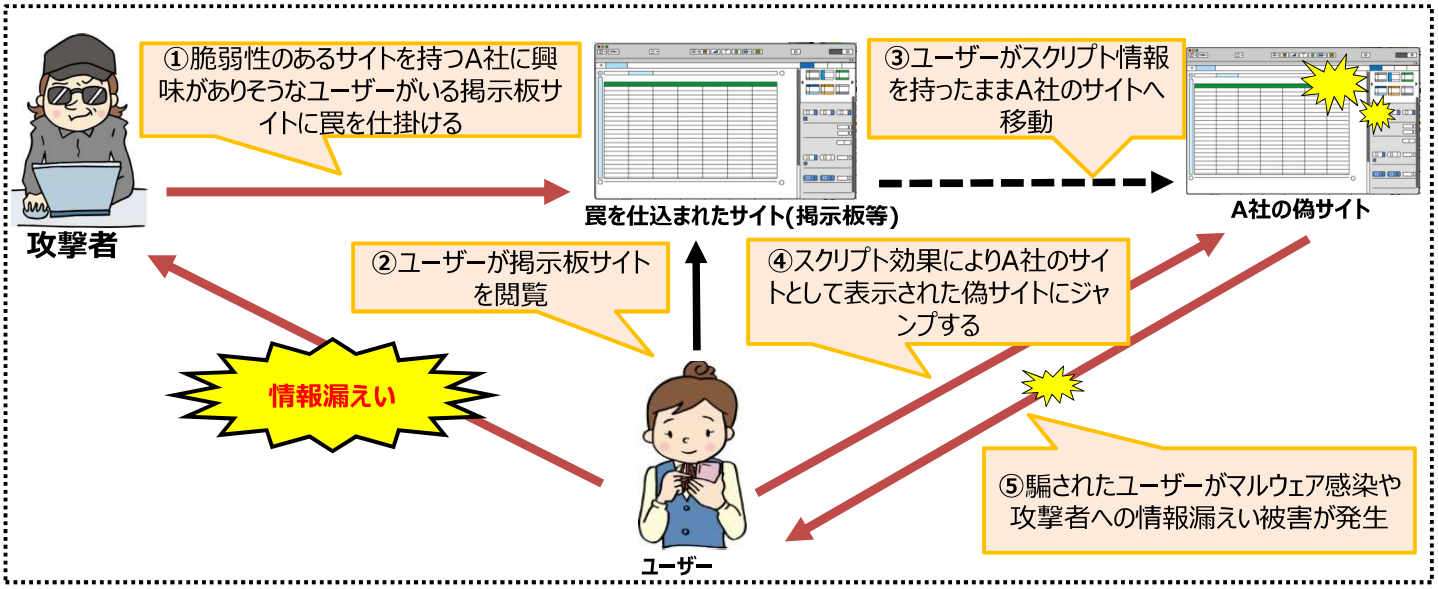
- 利用システムは稼働する前にソフトウェア・セキュリティプログラムのアップデートを行う等、セキュリティの検証を十分に行う。
- VPN機器経由にてリモート環境から社内システムへアクセスする際には、多要素認証を導入することで、万が一IDとパスワードが漏えいした場合であっても、なりすましによる不正アクセス被害を防ぐ。

29

Ⅴ.不正アクセスの具体事例

3.Webサイトへの攻撃（クロスサイトスクリプティング）

➢ インターネット掲示板などのWebサイトの記述言語であるHTMLに、悪質なサイトへ誘導するスクリプト(コンピュータプログラム)を仕掛けることで、攻撃対象になったwebサイトに訪れたユーザーの個人情報が搾取されてしまう事例が増えている。



【対策例】

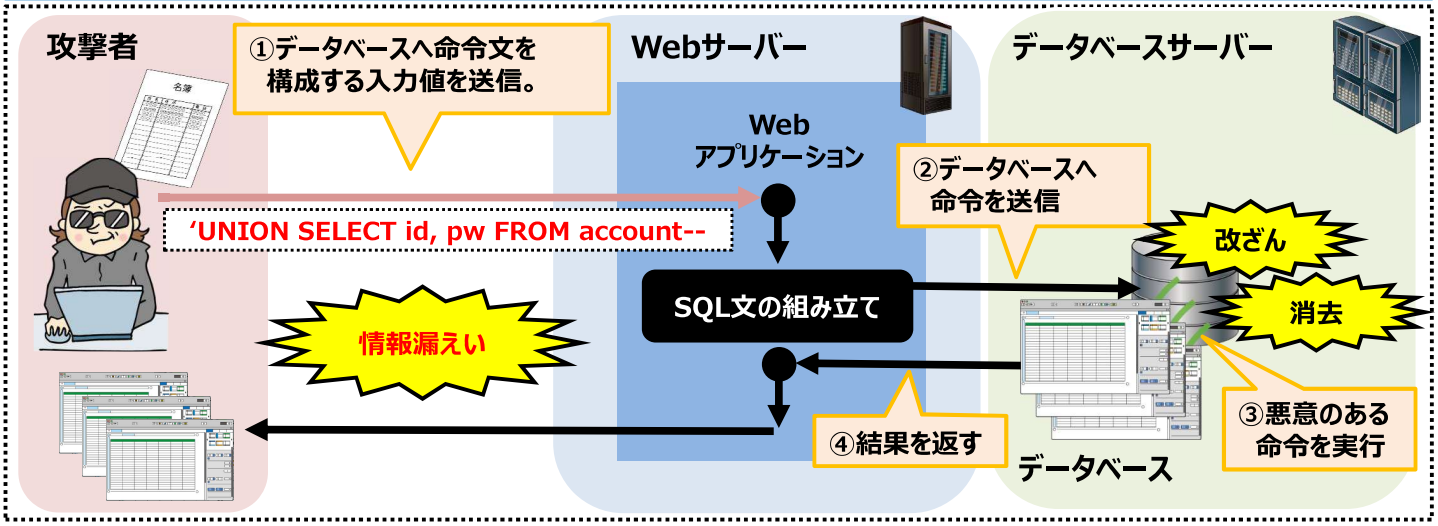
- WAF（Web Application Firewall）というWebアプリケーションを対象とした攻撃を検知･防御するセキュリティ製品を導入する。
- HTMLの出力要素にエスケープ処理を施し、攻撃者が意図したスクリプトが実行されないよう無害化する。

30

Ⅴ.不正アクセスの具体事例

4.サーバー攻撃による不正アクセス（SQLインジェクション攻撃）

➢ Webサイトに登録されている機密情報はデータベースに格納されているが、このデータベースを操作する際に 使用するSQL文の構造上の欠陥を悪用し、本来入力としては使われることが想定されていないSQL文を挿入 することで、データベースに格納されている商品情報やユーザー情報が漏えいする事例が増えている。



【対策例】

- SQL文の組み立ては全てプレースホルダで実装する。
  - ーSQL文の雛型の中に変数の場所を示す記号（プレースホルダ）を置いて、後にそこに実際の値を機械的な処理で割り当てる。
- SQL構文のすべての変数をエスケープ処理する。
  - ーSQL文中で可変となる値をリテラル（定数）の形で埋め込む

31

Ⅵ　今後、警察庁との連携を実施していくにあたり期待すること

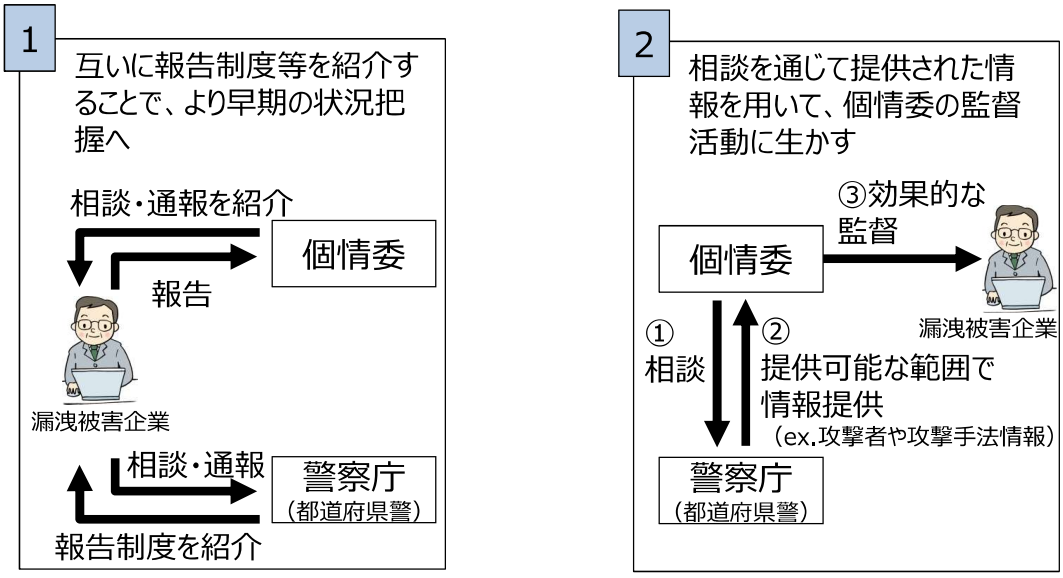
32

Ⅵ．警察庁との連携検討において期待すること

今後、警察庁との連携を実施していくにあたり、期待することは主に次の２つ。

1．漏えい等被害企業に対して、個情委と警察庁が相互に報告等の制度を紹介

2．サイバー攻撃における攻撃手法や有効な対策等に関する情報や調査結果等を受領



なお、各都道府県警察からの問合せについては、従来の個人情報保護法相談ダイヤル経由ではなく、当委員会において監視・監督業務を所掌する窓口へ直接連絡する運用へR4年11月から変更し、可能な部分から具体的な連携を進めているところ。

33

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

医療分野におけるサイバーセキュリティ被害の実態とセキュリティ上の課題

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室

Ministry of Health, Labour and Welfare of Japan

医療分野におけるサイバーセキュリティ被害の実態
－大阪府立病院機構 大阪急性期・総合医療センターのランサムウェア感染に関して－

事案概要

2022年10月31日(月) 早朝、地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター（以下、大阪急性期・総合医療センター）において、ランサムウェアを用いたサイバー攻撃によりファイルが暗号化され、電子カルテが使用不能となる事案が発生した。厚生労働省から派遣した初動対応支援チーム（一般社団法人ソフトウェア協会）の調査によると、感染経路は、院外の調理を委託していた給食事業者のシステムを経由したものである可能性が高いことが判った。

新規外来患者の受入は引き続き停止しているが、緊急度の高い処置、手術は大阪急性期・総合医療センターにおいて継続して対応している。緊急度の低い患者については、一度自宅退院、周辺病院への転院を進めたので、患者の生命等への影響はなかった。また、個人情報の漏洩も確認されていない。 （12月12日時点）

(参考)地方独立行政法人大阪府立病院機構 大阪急性期・総合医療センター
病床数：865床（一般病床831床、精神病床34床）
病院機能：基幹災害拠点病院、高度救命救急センター、地域周産期母子医療センター、小児地域医療センター、地域医療支援病院、
地域がん診療連携拠点病院　他
延べ入院患者数：22.3万人（646人/日）
延べ外来患者数：29.5万人（1,268人/日）

経過

10月31日(月)：インシデント発生。大阪急性期・総合医療センターからの初動対応支援の要請を受け、厚生労働省より初動対応支援チームを派遣。
同日夜、記者会見により当該事案を公表。
11月４日(金)：予定手術を一部再開。
11月７日(月)：発生後一週間経過。当該事案の現状と今後の復旧計画について記者会見を実施。感染経路は、給食事業者に設置されたVPN装置を経由した可能性が高いことを公表。
11月10日(木)：電子カルテの一部が仮設環境により参照可能となり、三次救急患者の受け入れと小児救急診療の一部を再開。
11月17日(木)：仮設環境による参照が救急外来において可能となり、一般救急患者の受け入れが再開。
12月12日(月)：電子カルテ再構築を完了させ本環境で順次稼働開始。各種オーダも順次再開予定。
来年１月：システム全面復旧予定

厚生労働省の対応

１．医療機関から要請を受けて、厚生労働省から専門家を派遣し、感染原因の特定や対応の指示等といった初動対応の支援を行った。
２．11月10日に全国の医療機関に対して、サイバーセキュリティ対策の強化にかかる注意喚起を行った。

医療分野におけるサイバーセキュリティ対策の課題

課題　**※①から③は、「医療情報システムの安全管理に関するガイドライン（第5.2版）」において医療機関等に対し実施を求めている。**

①VPN 機器等の脆弱性対策

リモート接続するために利用される、SSL-VPN 装置の脆弱性を悪用し、医療機関のネットワークに不正侵入し、ランサムウェアに感染させる事例が複数発生していることから、対応策として、ソフトウエア、機器等に脆弱性がないか点検し、脆弱性を発見した場合は早急に対処することが求められる。

②適切なバックアップの実施・管理の徹底

サイバー攻撃による障害発生後、復旧対応に速やかに移行できるよう、平時からデータやシステムのバックアップを確実に行うこと。特に、重要なファイルは、数世代バックアップを複数の方式かつ定期的に取得すること。また、バックアップが正常に取得できているか妥当性を定期的に確認するほか、復元手順をあらかじめ整備しておくことが必要。

③緊急対応手順の作成と訓練の実施

医療サービスを提供し続けるためのBCPの一環として、災害及びサイバー攻撃等を“非常時”と判断するための基準、手順、判断者等及び正常復帰時の手順をあらかじめ定めておくことが必要。

④サプライチェーンリスク対策

自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施することが求められる。

⑤情報セキュリティ人材の育成・確保

情報の非対称性の改善を目的に、IT技術・情報セキュリティに精通した人材の育成・確保が重要。

⑥インシデントの早期発見・検知

サーバ等における各種ログを確認するほか、通信の監視・分析やアクセスコントロールを再点検することが必要。

2

医療分野におけるサイバーセキュリティ対策

令和４年９月５日健康・医療・介護情報利活用検討会
医療等情報利活用ワーキンググループ資料２－２（一部改編）

予防対応

① 医療機関向けサイバーセキュリティ対策研修の充実

– 「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」において、**医療従事者や経営層等へ階層別のサイバーセキュリティ対策に関する研修の実施**や、本事業において作成される**ポータルサイトを通じた研修資材の提供**により、医療従事者や経営層等のサイバーセキュリティ対策の意識の涵養を図る。

② 脆弱性が指摘されている機器・ソフトウェアの確実なアップデートの実施

– 医療法第25条第１項の規定に基づく**立入検査の実施により確認**を行う。また、例年発出している「医療法第25条第１項の規定に基づく立入検査の実施について」（医政局長通知）において、令和４年度は**サイバーセキュリティ対策の強化に関する事項について記載**した。**令和４年度中に医療機関等の管理者が遵守すべき事項に位置付けるための省令改正**を行う。

– NISCより情報提供のあった脆弱性情報について、医療セプターを通じた情報提供を引き続き行う。

③ 医療分野におけるサイバーセキュリティに関する情報共有体制（ISAC）の構築

– 他分野のISAC関係者の協力を得つつ、医療関係者数名のコアメンバーによる**検討グループを年内に立ち上げる。**

④ 検知機能の強化

– **不正侵入検知・防止システム（IPS／IDS）の設置・活用を進める**よう、医療情報システムの安全管理に関するガイドライン**改定の検討**を行う。

⑤ G-MISを用いた医療機関への定期調査の実施

– 医療機関に対する**サイバーセキュリティ対策の実態調査**を令和４年度中に実施する。

【質問項目（例示）】
・医療法に基づく立入検査の留意事項を認識し、必要な措置を講じているか。
・（許可病床数が400床以上の保険医療機関に対して）診療録管理体制加算の見直しを受けて、専任の医療情報システム安全管理責任者を配置しているか。

3

医療分野におけるサイバーセキュリティ対策

初動対応

① インシデント発生時の駆けつけ機能の確保

– 200床**以下**の医療機関に対し、**サイバーセキュリティお助け隊の活用を促進するための周知・広報**を行う

– 200床**以上**の医療機関に対し、「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」において、**サイバーセキュリティインシデントが発生した医療機関の初動対応支援**を行う。

② 行政機関等への報告の徹底

– **医療情報セキュリティ研修およびG-MIS調査を通じ**、医療情報システムの安全管理に関するガイドラインに基づいた**厚生労働省への報告の徹底**や、個人情報保護法改正に伴う**個人情報保護委員会への報告義務化の周知**を図る。

– 厚生労働省より、医療情報システムの安全管理に関するガイドラインに基づいて医療機関より報告のあったサイバーインシデント事案について、攻撃先が同定されない程度に報告内容を適時情報提供し、攻撃手法や脅威について分析を行い、全国の医療機関へ情報発信・注意喚起を行う。

復旧対応

① バックアップの作成・管理の徹底

– 医療情報セキュリティ研修およびG-MIS調査を通じ、**バックアップの具体的な作成が明記**された医療情報システムの安全管理に関するガイドライン（５．２版）の周知を行う。

– 令和３年６月28日発出「医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)」の記載事項に留意し、データ・システムのバックアップを行う。

– 令和4年度診療報酬改定における診療録管理体制加算に係る報告書（７月報告）により、**バックアップ保管に係る体制等の確認**を行う。

② 緊急対応手順の作成と訓練の実施

– 「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業一式」において、**サイバーセキュリティインシデントが発生した際の対応手順の調査**を行い、**適切な対応フローの整理**を行う。また、整理した対応フローをもとに**サイバーセキュリティインシデントに備えたBCPの提案**を行う。

その他

「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」の対象事業者と医療機関等の合意形成の項目及び、HELICS協議会において医療情報化指針として採択した（令和4年8月）「製造業者/サービス事業者による医療情報セキュリティ開示書」（MDS/SDS）の遵守を業界団体及び医療機関に徹底する。

4

医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業（令和４年度）

背景

医療分野のサイバーセキュリティについては、近年その脅威が高まっていることから、令和４年度厚生労働省事業において、医療機関向け研修やサイバーセキュリティインシデント発生時の初動対応の支援等を行う。

事業概要

（１）サイバーセキュリティ対策にかかる医療機関向け研修の実施
：医療機関職員の階層（初学者、経営層、システム･セキュリティ管理者等）に応じた研修の実施

（２）継続的な教育支援
：医療情報システム安全管理者が研修に活用できる教育コンテンツ作成･収集と公開

（３）平時のサイバーセキュリティインシデント対応手順の調査および既存BCPの見直し提案
：サイバーセキュリティインシデント発生時の適切な対応フローの整理、BCP（Business Continuity Plan）の提案

（４）サイバーセキュリティインシデントが発生した医療機関の初動対応支援
：サイバーセキュリティインシデントが発生した医療機関の原因究明や早期診療復帰を目的に、初動対応支援を実施

受託者

一般社団法人　ソフトウェア協会
：約700社のソフトウェア製品に係わる企業が集まり、ソフトウェア産業の発展に係わる事業を通じて、我が国産業の健全な発展と国民生活の向上に寄与することを目的とした一般社団法人
（サイバーセキュリティに関する主な活動内容）
・ソフトウェアやサイバーセキュリティに関連したセミナー、研修の実施　・サイバーセキュリティに関する情報交換・周知
・サイバーセキュリティボランティア制度の創設・運用

5

医療業界と警察との連携体制

令和3年12月17日　第８回健康・医療・介護情報利活用検討会
医療等情報利活用ワーキンググループ警察庁講演資料引用

- 令和２年８月21日　富山県公的病院長協議会と富山県警が「サイバー犯罪被害防止の取組に関する協定」を締結

県内の公立・公的病院と、**被害の未然防止につながる知見・情報の共有を更に深化させることで、医療機関を対象としたサイバー犯罪の発生を防ぐ**ことにより、県民が安心して暮らせる社会の実現を図る

（出典：日刊警察　https://nikkankeisatsu.co.jp/news/200908-1.html）

- 他の都道府県警察においては、各種事業者等で構成される協議会を設置し、サイバーセキュリティに関する情報共有を実施

6

クレジットカード決済における
サイバーセキュリティ事案の犯罪抑止に向けて

令和４年12月12日

経済産業省

目次

１．クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）

２．クレジットカード決済でのサイバーセキュリティ上の被害実態

３．今後、警察庁との連携の実施にあたり期待すること

1．クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）

2

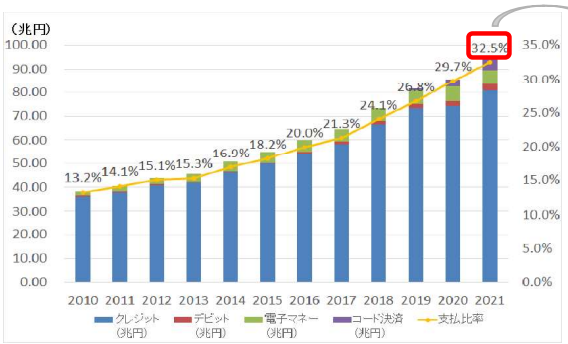
1．背景

経済産業省HP　クレジット・セキュリティ対策ビジョン2025第1.1版より引用

キャッシュレス決済の伸長

国内キャッシュレス決済額・比率は順調に増加（うちクレジットカード取引は約９割）

キャッシュレス支払額及び決済比率の推移



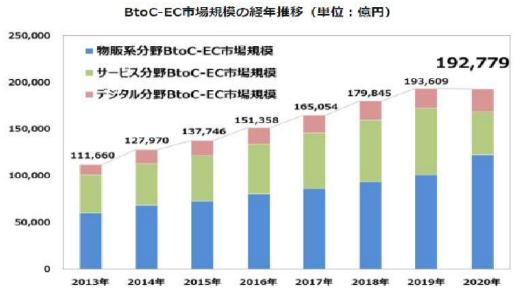
2025年6月まで
40%
※目標値

うちクレジット：
約100兆円
※見込み

出典：経済産業省HP

EC決済サービスの伸長

EC取引の伸長に伴って、消費者のクレジットカード番号の入力機会が増加



2021年
EC市場規模
約19兆円

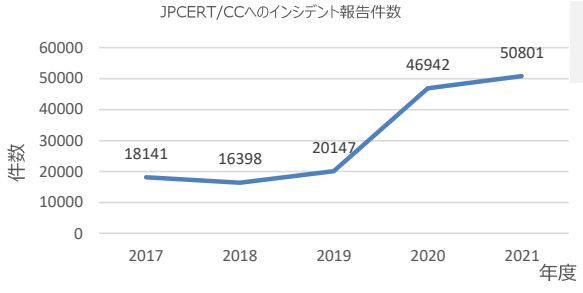
出典：令和2年度産業経済研究委託事業（電子商取引に関する市場調査）経済産業省

参考：民間(矢野経済研究所)の試算によると、キャッシュレス決済額全体は2025年に約**150**兆円まで拡大するとされている

参考：民間(SBペイメント)の試算によると、EC決済のうち約 **8** 割はクレジットカードを使った決済が行われている

サイバーセキュリティインシデントの発生

全業種的にサイバーセキュリティインシデントへの脅威が高まっている

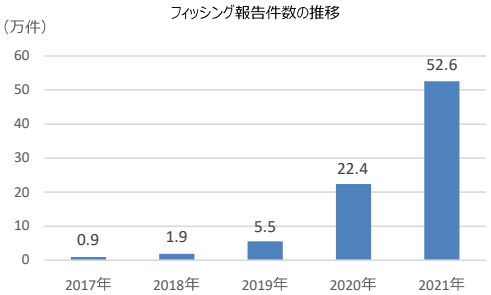


2021年度
報告件数
約５万件

出典：JPCERT/CCインシデント報告対応レポート（2022年４月14日）

フィッシング被害の増加

近年、消費者を狙ったフィッシングの報告件数も急増



2021年
フィッシング報告件数
約53万件

フィッシングとは：
メールやSMSを通じて、個人情報等（クレジットカード番号等を含む）をだまし取ること

出典：JC3HP（フィッシングターゲットの変遷）

3

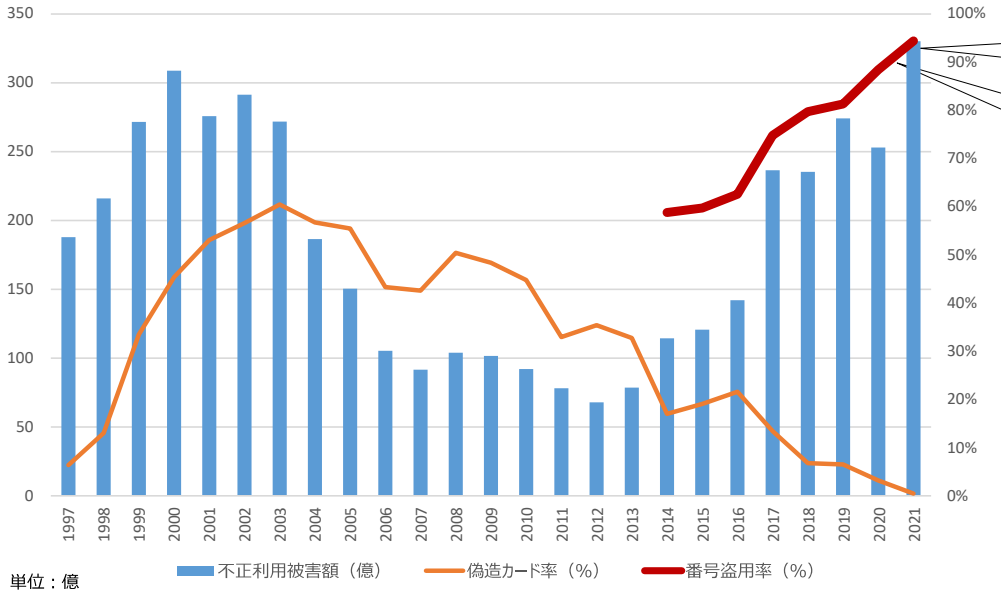
1．クレジットカードにおける不正利用被害

経済産業省HP　クレジット・セキュリティ対策ビジョン2025第1.1版より引用･改変

結果として、不正利用被害額は過去最高に、そのうち番号盗用被害額も過去最高に

※　サイバー攻撃やフィッシング等によって漏えい･割り出されたクレジットカード情報を用いて、クレジットカードによる不正利用に使われている

国内発行クレジットカードにおける年間不正利用被害額推移



単位：億

2021年における不正利用被害**総額**
330億円

2021年の不正利用被害総額に対する**番号盗用**の被害割合
94%

想定される番号盗用の原因
- 加盟店等、事業者からの漏えい
- フィッシング
  （メールやSMS等を通じて、利用者からクレジット情報等をだまし取る）
- クレジットマスター（クレジットカード番号自体は盗まず、他人のクレジットカード番号から確率的に割り出す手法）

出典：日本クレジット協会（令和４年３月）

補足：ダークウェブでのクレジットカード番号等の取得による不正利用

※　盗まれたクレジットカード情報は、ダークウェブ等において売買され、不正利用に使われることもある

事案１）クレジットカードの情報をダークウェブで入手し、高級腕時計を購入し売却したとして逮捕
事案２）クレジットカードの情報をダークウェブで購入し悪質事業者に売りさばいたとして学生を逮捕

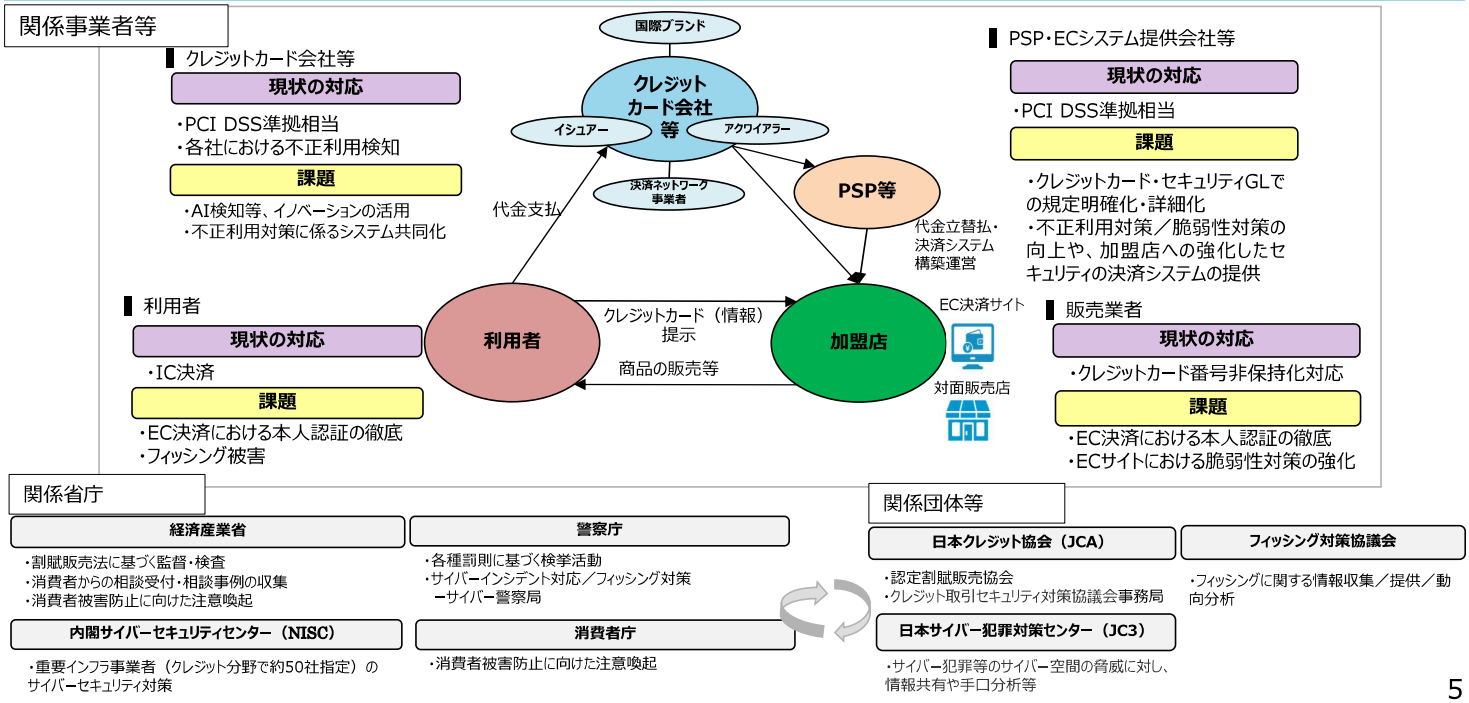
参考：民間セキュリティ会社の調査によると、日本のクレジットカード情報は闇サイトで平均約5200円で販売されているとの情報も（2022/4/4　共同通信社）

4

1．クレジットカードシステムのセキュリティ対策の現状と課題

経済産業省HP　クレジット・セキュリティ対策ビジョン2025第1.1版より引用

- 加盟店と利用者との決済サービスをクレジットカード会社が提供するという基本的関係をもとに様々な事業者が参画。
- クレジットカードシステムに対するセキュリティは、
  ① 当初は、**クレジットカード会社**によるPCI DSS準拠等の漏えい防止対策。
  ② 一方、キャッシュレス決済の広まりに伴い、**利用者**や**加盟店**といったフロントでの対策も重要。
  ③ 最近では、**決済代行業者（PSP）等**の、クレジットカード会社と加盟店の間にいる事業者が決済情報を集積している場合も多く、これらの事業者におけるさらなるセキュリティ対策強化が課題と認識。
- 今後は、関係事業者･関係省庁･関係団体等の連携がより一層重要になる。



5

1．クレジットカード番号セキュリティ対策の３つの方向性

クレジットカード会社等　加盟店　利用者　PSP等

目的意識	これまでの取組	今後の方向性
クレジットカード番号を安全に管理する（漏えい防止）		
▌クレジット決済に関与するプレイヤーは、クレジットカード番号を取り扱う上でシステム等の安全性を確保する	✓ 割賦販売法に基づく対応（クレジットカード番号等の適切管理規定） － PCI DSS準拠相当 － 非保持化	✓ さらなる制度的措置の検討 ークレジットカード・セキュリティガイドラインでのアップデート ✓ 加盟店やPSP等のECサイト、システムの脆弱性対策の強化
クレジットカード番号を不正利用させない（不正利用防止）		
▌決済を承認する際には本人認証を行い、なりすましをさせない	✓ 割賦販売法に基づく対応 － 対面取引におけるIC決済の推進 － 非対面取引における本人認証の導入（セキュリティコード・静的パスワード等における認証）	✓ 特に非対面取引における本人認証の原則化 ✓ 本人認証方法の高度化 生体認証・ワンタイムパスワード等といった強力な本人認証方法を推進 ⇒EMV-3Dセキュアの普及
▌決済取引をモニタリングし、不正利用を検知する	✓ クレジットカード会社等における個社での不正検知の取組 ✓ 明細、利用履歴の確認（クレジットカード会社等における明細通知・利用者における確認）	✓ 共同システムの構築・新しい技術や方法に基づく不正利用検知のイノベーション ✓ 明細による確認強化（リアルタイム通知等、利用者へのアラート機能の充実）
クレジットの安全・安心な利用に関する周知・犯罪の抑止		
▌利用者は、悪意を持った第三者からのフィッシング被害に遭わないよう対策を行う	✓ フィッシング対策協議会や日本クレジット協会等における周知啓発	✓ フィッシング対策に向けた多層的な取組（送信ドメイン認証（DMARC）等） ✓ 周知啓発の強化 ✓ 事業者と行政機関等における連携強化
▌漏えい防止・不正利用防止で行き届かない部分については、執行で対応	✓ 割賦販売法第49条の２（クレジットカード番号の不正利用・取得）／不正アクセス禁止法等に基づく執行対応	✓ 経済産業省と警察庁（サイバー警察局等）との連携強化

6

1．安全・安心なクレジットカード決済環境の進展と今後のロードマップ（イメージ）

経済産業省HP　クレジット・セキュリティ対策ビジョン2025第1.1版より引用

7

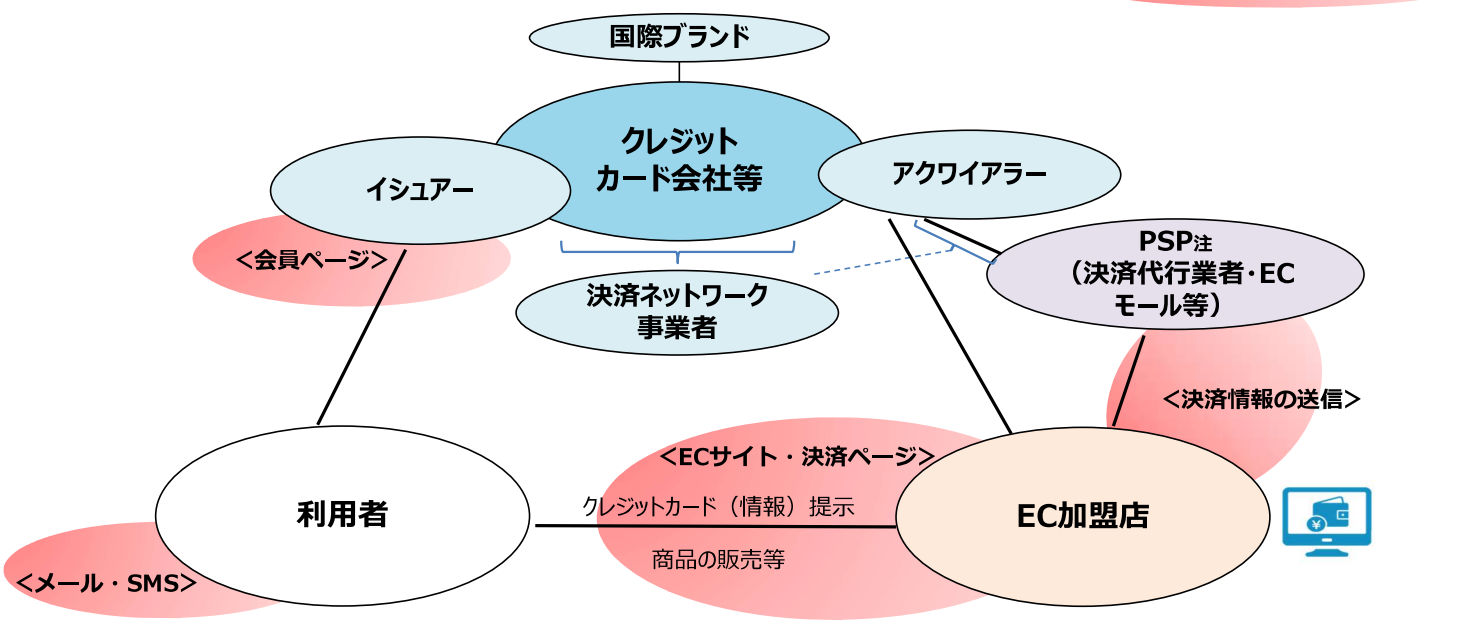
2．クレジットカード決済でのサイバーセキュリティ上の被害実態

8

クレジットカード番号等の漏えいリスク

- クレジットカード決済システムは、多数の事業者のネットワークによって成立。クレジットカード番号を直接保持（保存・処理・通過）しているプレイヤーだけでなく、インターネットを介してクレジット決済を可能にするネットワークの接続を持つプレイヤーにも常にサイバー攻撃のリスクが存在。

サイバー攻撃による漏えいリスクのイメージ図

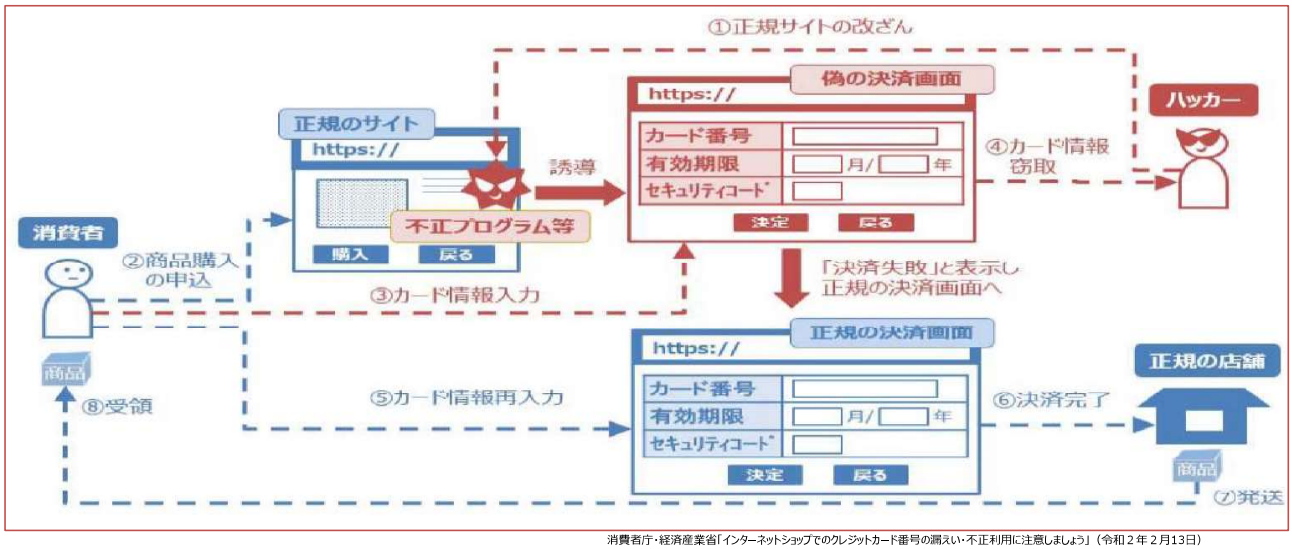


注：本資料では、PSPをその機能面から「インターネット上の取引において EC 加盟店にクレジットカード決済スキームを提供 し、カード情報を処理する事業者」とする。

9

漏えい事案①－１：EC加盟店

- 特にオープンソースにより構築され、自社（委託先含む）で適切なアップデートを行わないなど、十分なセキュリティ対策を講じていないECサイトの脆弱性を狙った不正アクセス等による漏えい事案が増加。クレジットカード番号等を保持していなくとも、**ECサイト自体が改ざんされることで、不正ファイルの設置や偽の決済サイトへの誘導でクレジットカード番号等が流出。**
- 当省でも加盟店に対する注意喚起を実施(令和元年12月）。IPAとも連携。
- しかしながら、**ECサイトでのサイバー攻撃によるクレジットカード番号漏えい事案は増加**（約２割増（うちオープンソース関連は、約４割増加））。



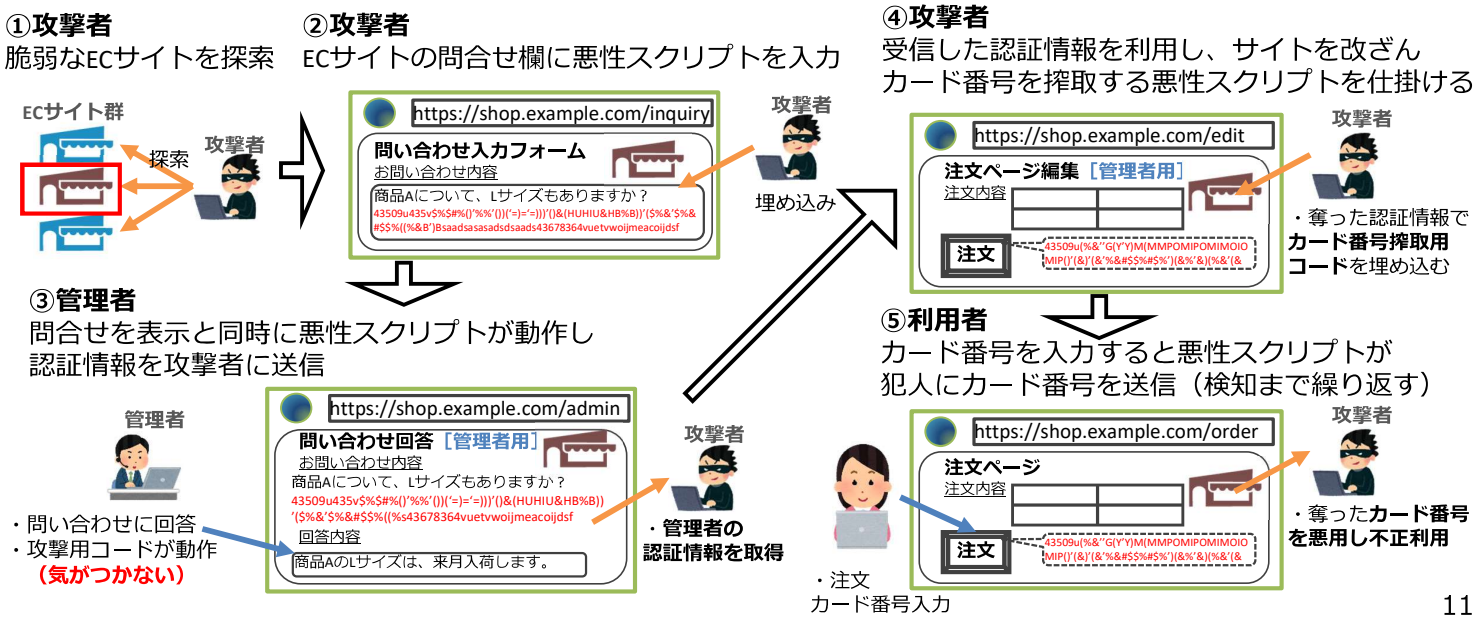
消費者庁・経済産業省「インターネットショップでのクレジットカード番号の漏えい・不正利用に注意しましょう」（令和２年２月13日）
https://www.caa.go.jp/policies/policy/consumer_policy/caution/internet/pdf/consumer_policy_cms104_200218_01.pdf

10

（参考）漏えい事案①－１：EC加盟店（サイバー攻撃手法）

- 昨今のEC加盟店での漏えいは主として既知のサイバー攻撃による。その多くが、外部のインターネットと接続している問合せフォームや注文サイト等へのクロスサイトスクリプティングにより、ECサイトを改ざんし、データを搾取するもの。
- 特に利用者の多いECパッケージでは、攻撃側に脆弱性を熟知されており、攻撃側にとって、より効率的に攻撃できることから、攻撃の対象となりやすい。

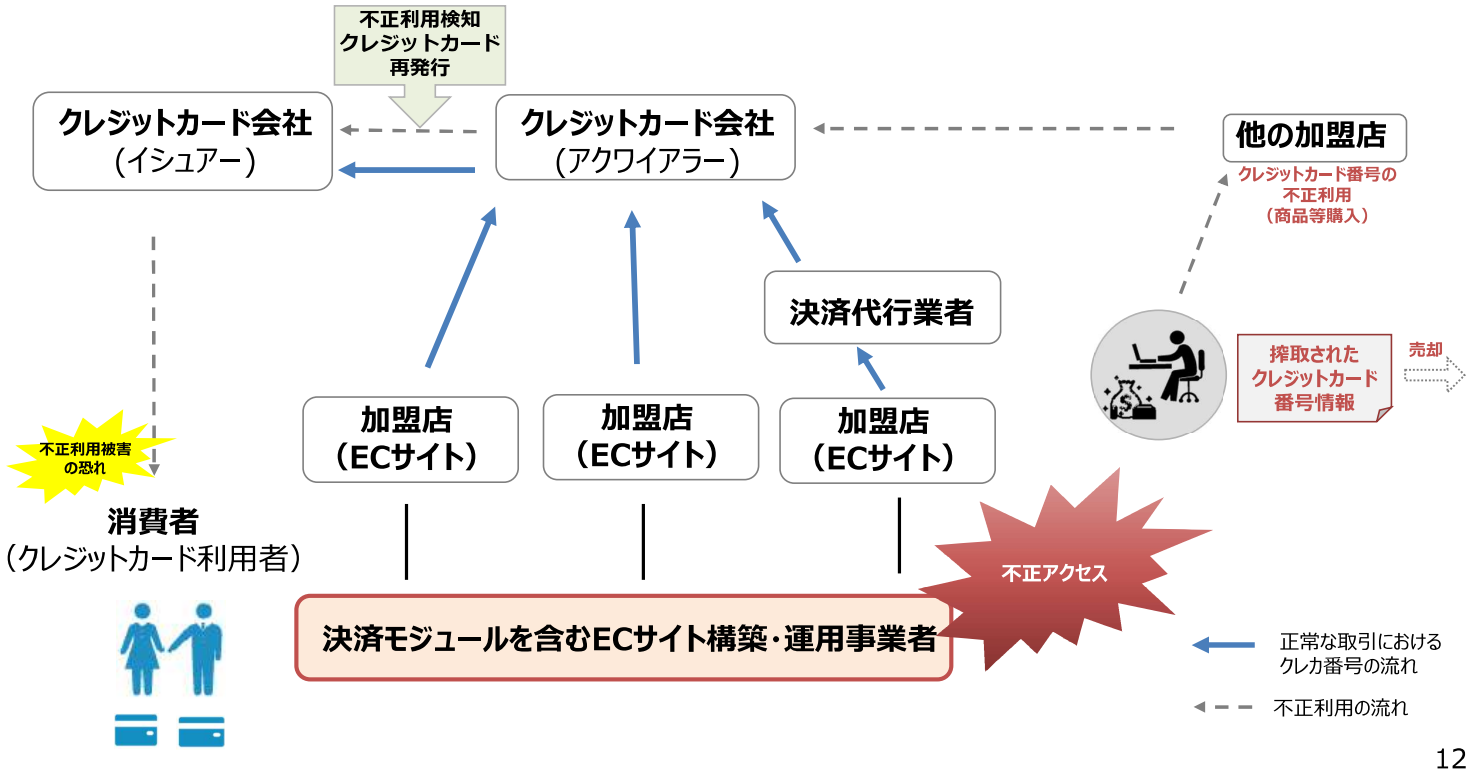
EC加盟店へのサイバー攻撃のイメージ



11

漏えい事案①－２：ECシステム提供者

- EC加盟店での漏えいは、決済モジュールを含むECサイトを構築・運用する事業者のサーバーへの不正アクセスを起因とするものも発生。この場合、**一事案であっても、漏えいの規模が広くなる**（関連するEC加盟店は約９事業者）。

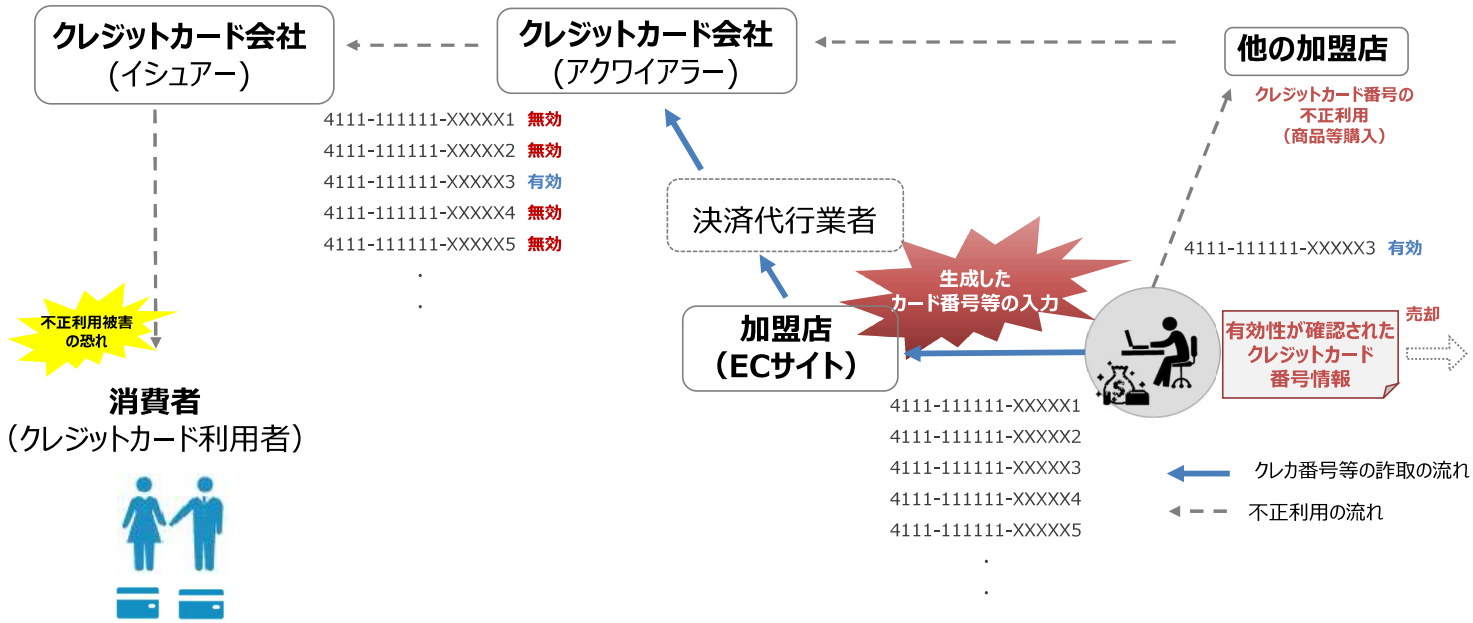


12

月村0

漏えい事案１－③：クレジットマスター（有効性確認）

- EC加盟店からの決済ネットワークを通じて、**機械的に生成した多量のクレジットカード番号等の有効性を確認**することにより、有効なカード番号等を割り出す手法。
- 無効なクレジットカード番号等であっても、大量の有効性確認用の決済処理のコストがEC加盟店に発生する。



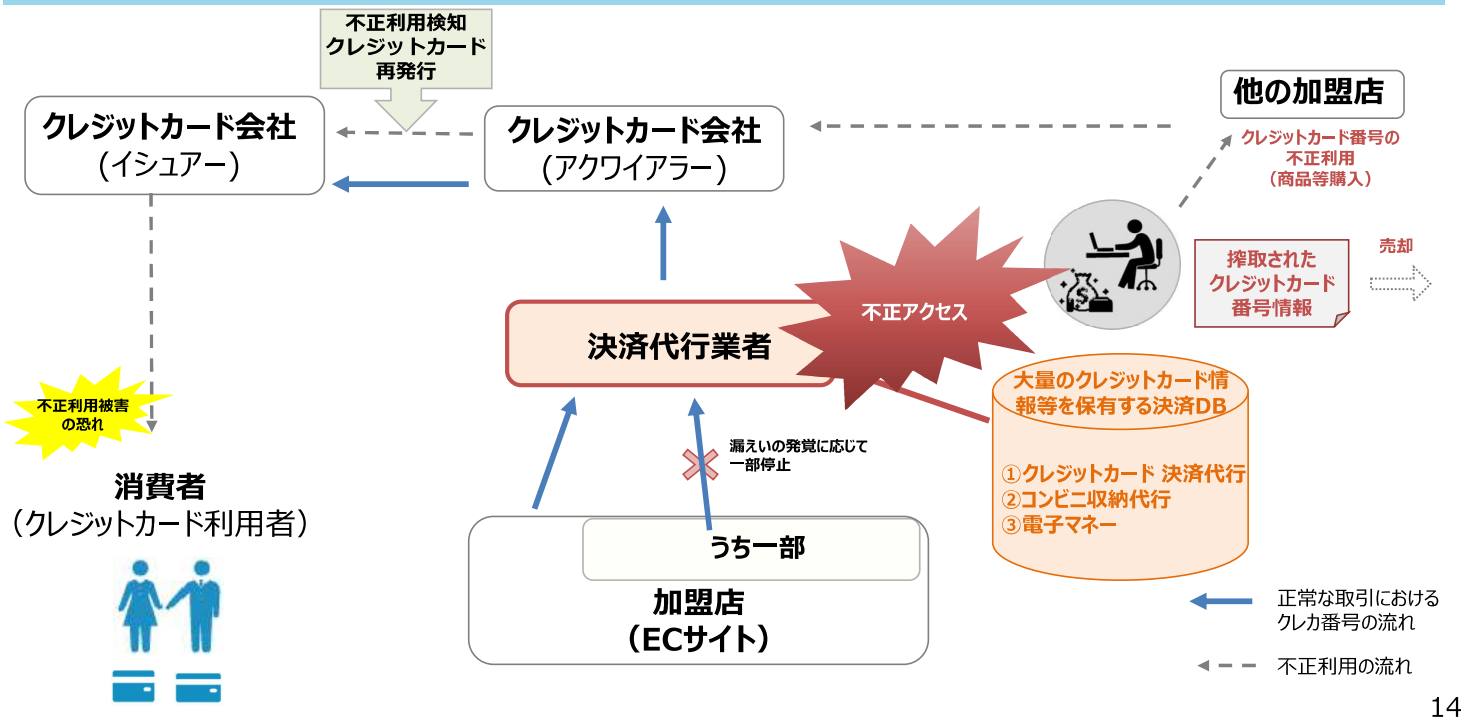
13

スライド 14

月村0　（今後備忘）
・クレマスの位置付け　漏えいで良いはずだが課長に念押し
・漏えいは１事業者（EC加盟店、PSP、クレマス）/２消費者（フィッシング）の整理
月村, 2022-12-12T01:28:46.088

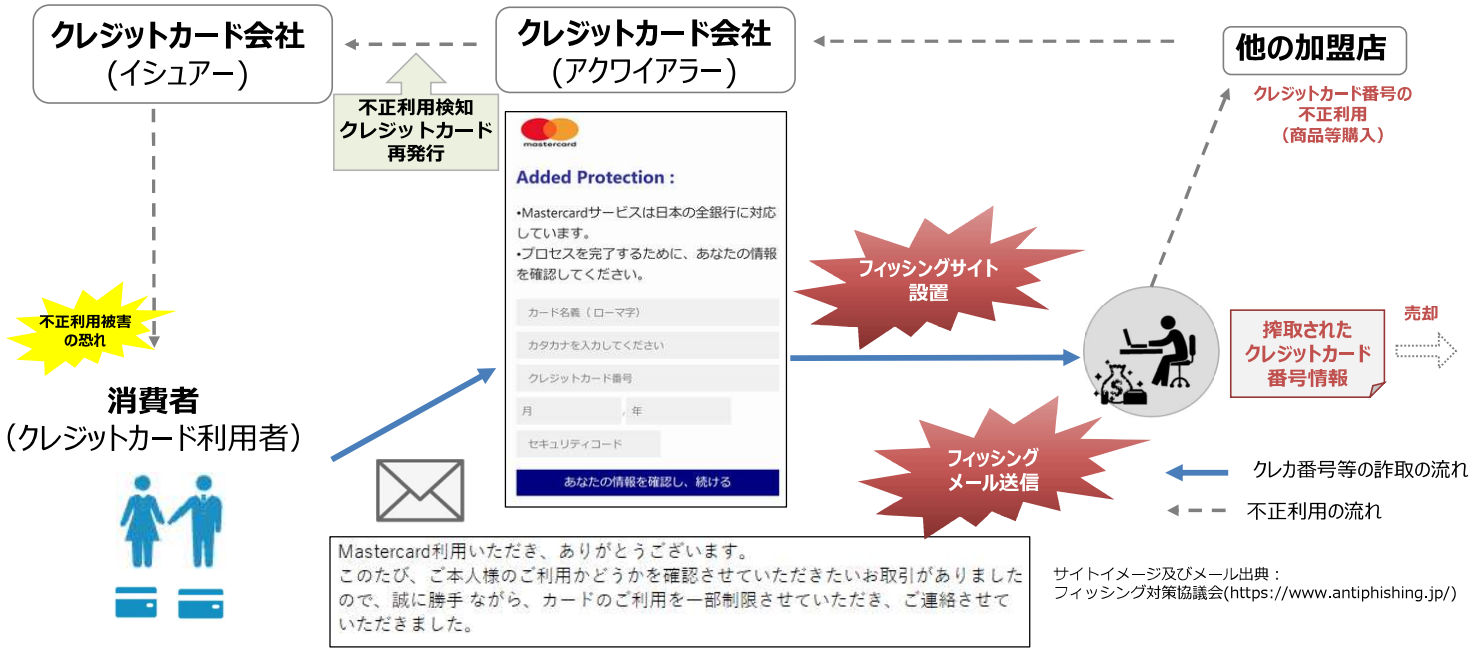
漏えい事案②PSP(決済代行業者)

- クレジットカードの決済代行業者の**大量の情報を保有するデータベース**（約46万件のクレジットカード番号等を含むトークン方式クレジットカード決済情報データベース、約240万件のクレジットカード番号等が含まれる決済情報データベース）**への外部からの不正アクセス**により、同社が運営する複数の決済サービスにおいて、決済情報の大規模な漏えいが発生。令和２年割賦販売法改正後、初めての事案。



漏えい事案③消費者（フィッシング被害）

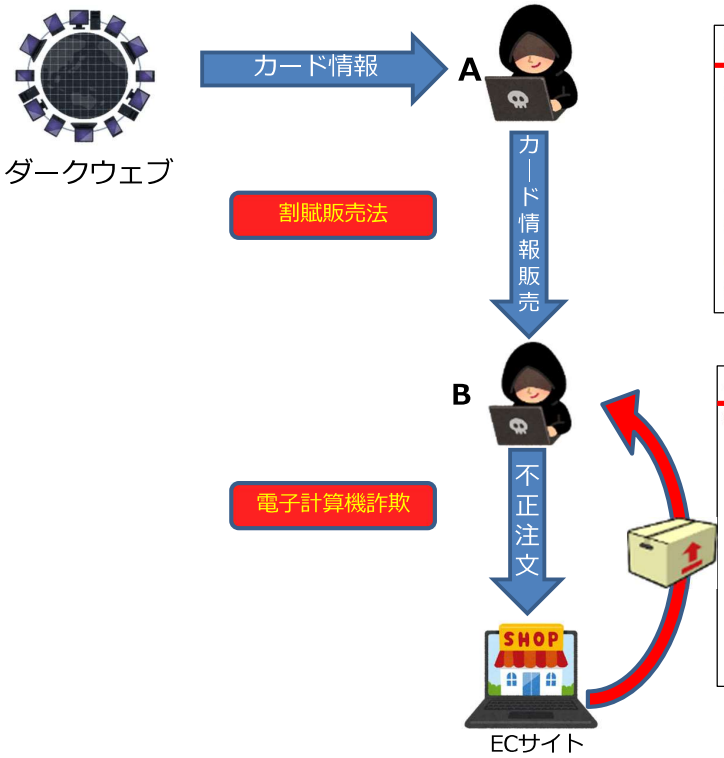
- サイバー攻撃によるクレジットカード番号盗用以外にも、**消費者自身が偽サイトにクレジットカード番号やID・パスワード等を入力する**フィッシングによるクレジットカード番号等の漏えい事案も存在。



サイトイメージ及びメール出典：
フィッシング対策協議会(https://www.antiphishing.jp/)

15

不正利用事案①クレカ番号等の売買・不正利用



クレカ情報販売、学生を再逮捕　割賦販売法違反の疑い

2022年4月13日 2:00 [有料会員限定]

保存

インターネット上で不正入手したクレジットカード情報を第三者に販売したとして、愛知県警などは12日、ブラジル国籍で三重県四日市市の大学生、パシェコ・ビクトール・モアヅキ容疑者（21）=電子計算機使用詐欺罪などで起訴=を割賦販売法違反の疑いで再逮捕した。1万2千件以上のカード情報...

引用元：日本経済新聞2022年4月13日版

クレジットカード情報購入　容疑の男逮捕　静岡県警など

2022.8.24

静岡、愛知など８県警の合同捜査本部は２３日、割賦販売法違反の疑いで沖縄県宜野湾市大謝名５丁目、建築作業員の男（２１）を逮捕した。

容疑者は購入したカード情報を悪用し、少なくとも約１７３万円分の買い物をしていたとみられる。不正入手したカード情報などを転売する事件に絡む捜査の中で、容疑者が浮上した。

引用元：静岡新聞2022年8月24日版

（出典）第4回クレジットカード決済システムのセキュリティ対策強化検討会資料4（警察庁提出）

16

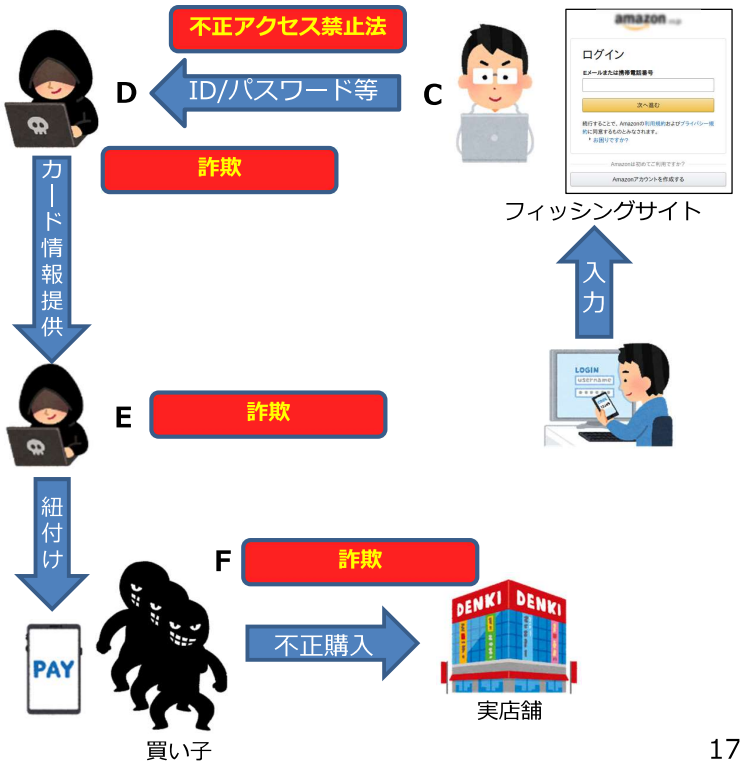
不正利用事案②フィッシング・不正利用

ｄ払い詐欺、指示役逮捕　容疑で愛知県警など、組織的に不正か

2021年10月6日 23時24分 (10月6日 23時28分更新)

ＮＴＴドコモのスマートフォン決済サービス「ｄ払い」を不正利用して買い物をするよう指示したとして、愛知、徳島両県警の合同捜査本部は６日、詐欺の疑いで名古屋市千種区富士見台１、無職古屋十兵容疑者（２６）を逮捕した。捜査本部はこれまでに実行役５人を逮捕しており、古屋容疑者らの指示の下、組織的に不正利用を繰り返していたとみて調べている。

引用元：中日新聞2021年10月6日版



（出典）第4回クレジットカード決済システムのセキュリティ対策強化検討会資料4（警察庁提出）

３．今後、警察庁との連携の実施にあたり期待すること

3．クレジットカード番号セキュリティ対策の３つの方向性（再掲）

クレジットカード会社等　加盟店　利用者　PSP等

目的意識	これまでの取組	今後の方向性
クレジットカード番号を安全に管理する（漏えい防止）		
▌クレジット決済に関与するプレイヤーは、クレジットカード番号を取り扱う上でシステム等の安全性を確保する	✓ 割賦販売法に基づく対応（クレジットカード番号等の適切管理規定） － PCI DSS準拠相当 － 非保持化	✓ さらなる制度的措置の検討 ークレジットカード・セキュリティガイドラインでのアップデート ✓ 加盟店やPSP等のECサイト、システムの脆弱性対策の強化
クレジットカード番号を不正利用させない（不正利用防止）		
▌決済を承認する際には本人認証を行い、なりすましをさせない	✓ 割賦販売法に基づく対応 － 対面取引におけるIC決済の推進 － 非対面取引における本人認証の導入（セキュリティコード・静的パスワード等における認証）	✓ 特に非対面取引における本人認証の原則化 ✓ 本人認証方法の高度化 生体認証・ワンタイムパスワード等といった強力な本人認証方法を推進 ⇒EMV-3Dセキュアの普及
▌決済取引をモニタリングし、不正利用を検知する	✓ クレジットカード会社等における個社での不正検知の取組 ✓ 明細、利用履歴の確認（クレジットカード会社等における明細通知・利用者における確認）	✓ 共同システムの構築・新しい技術や方法に基づく不正利用検知のイノベーション ✓ 明細による確認強化（リアルタイム通知等、利用者へのアラート機能の充実）
クレジットの安全・安心な利用に関する周知・犯罪の抑止		
▌利用者は、悪意を持った第三者からのフィッシング被害に遭わないよう対策を行う	✓ フィッシング対策協議会や日本クレジット協会等における周知啓発	✓ フィッシング対策に向けた多層的な取組（送信ドメイン認証（DMARC）等） ✓ 周知啓発の強化 ✓ 事業者と行政機関等における連携強化
▌漏えい防止・不正利用防止で行き届かない部分については、執行で対応	✓ 割賦販売法第49条の２（クレジットカード番号等の不正利用・取得）／不正アクセス禁止法等に基づく執行対応	✓ 経済産業省と警察庁（サイバー警察局等）との連携強化

（資料）クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）（第30回産構審割販小委（令和４年６月

19

3．クレジットカード決済システムのセキュリティ強化対策検討会

- 電子商取引及びキャッシュレス決済の普及に伴い、クレジットカード決済市場の規模が増加する一方、サイバー攻撃の増加等を背景に、クレジットカードの不正利用被害額が過去最高。また、クレジットカード決済機能の分化により多様なプレイヤーがクレジットカード決済網に関与していく傾向。
- これらの状況に鑑み、技術的観点も含めて、３つの方向性を踏まえながら、クレジットカード決済システムのセキュリティ対策強化に向けた具体的な取組について議論。令和５年年初を目途に取りまとめ予定。

【委員】
中川丈久 神戸大学法学研究科・法学部 教授 【座長】
池本誠司 日本弁護士会連合会消費者問題対策委員会 幹事
大河内 貴之 Ｓｅｃｕｒｅ・Ｐｒｏ株式会社 代表取締役
大野克巳 一般財団法人日本サイバー犯罪対策センター 経済・金融犯罪対策担当部長
小川睦世 一般社団法人日本クレジットカード協会 事務局長
篠寛 ＥＣ決済協議会 会長（株式会社ＤＧフィナンシャルテクノロジー 代表取締役社長共同ＣＯＯ 兼 執行役員ＳＥＶＰ）
二村浩一 山下・柘・二村法律事務所 弁護士
長谷川ゆかり 公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会
松尾健一 大阪大学大学院高等司法研究科 教授
三浦千宗 公益社団法人日本通信販売協会 理事 事務局長
森竹由美子 ＢＳＩグループジャパン株式会社 認証事業本部金融セクター部 部長

【オブザーバー】
日本クレジット協会
クレジット 取引 セキュリティ対策協議会
情報処理推進機構セキュリティセンター
警察庁サイバー警察局サイバー企画課
金融庁 資金決済モニタリング室
経済産業 省 商務情報政策局 サイバー セキュリティ 課

【議事】

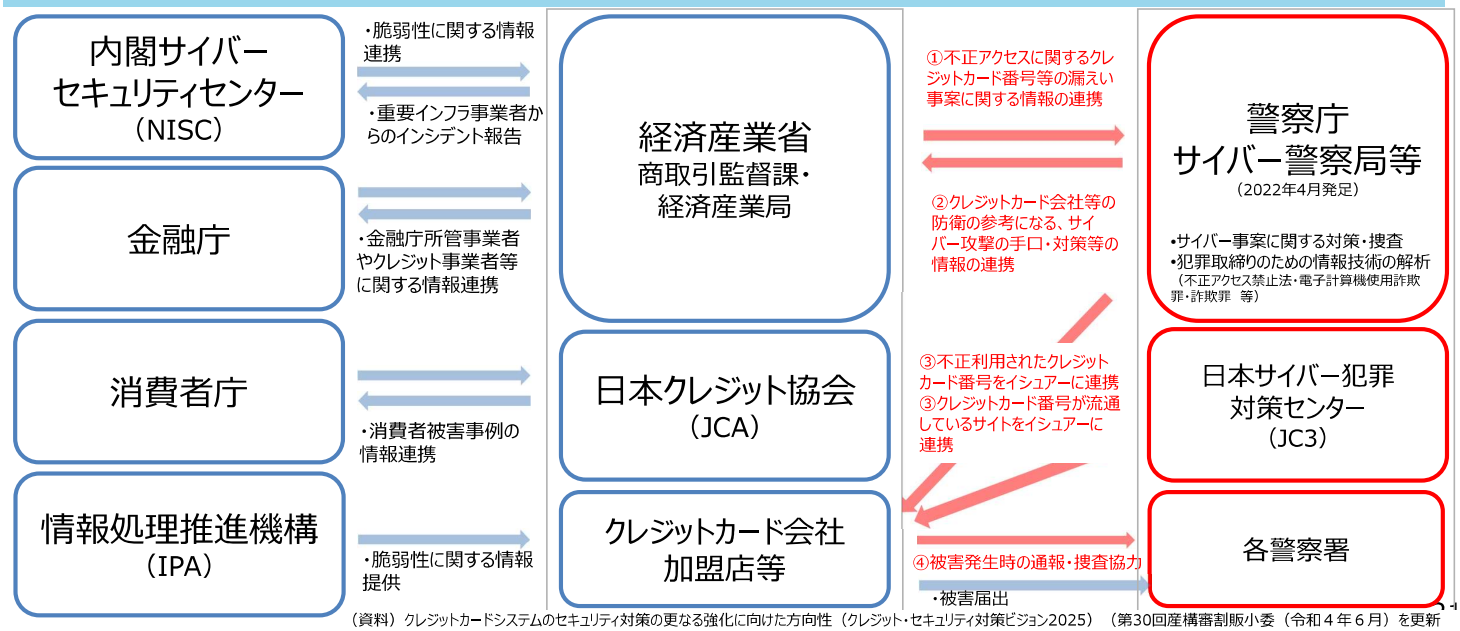
第１回（8月4日）
・自由討議
第２回（9月13日）
・クレジットカード番号等の漏えい対策
第３回（10月11日）
・クレジットカード番号等の不正利用対策
第４回（11月15日）
・クレジットの安全・安心な利用に関する犯罪の抑止（フィッシング対策、警察等との連携）
・クレジットカード番号等の漏えい対策（インシデント対応・漏えい防止にかかる利用者保護）
・クレジットの安全・安心な利用に関する周知
第５回（12月下旬予定）
・取りまとめ骨子案
第６回（1月予定）
・取りまとめ

20

３．犯罪抑止に向けた関係行政機関等との連携強化（サイバー犯罪）

赤枠・・・取組を強化している主体
赤矢印・赤字・・・新たな取組案
青矢印・黒字・・・これまでの取組

- 従来より、クレジットカード会社等はサイバー攻撃によるインシデント時に関係行政機関・団体への報告・相談を行うとともに、所管の警察署にも通報を行ってきた。
- 一方、昨今は、サイバー攻撃によるクレジットカード番号等の漏えいや不正利用等のサイバー犯罪が急増。
- 今後は、更に犯罪防止に資するべく、より詳細かつ実効的な情報共有を行うため、関係省庁・業界団体間での連携強化の構築も、対策として考えられる。



（資料）クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）（第30回産構審割販小委（令和４年６月）を更新