サイバー脅威の現状とJC3の取り組み

2018年1月6日@一橋講堂　1640-17:30
第6回情報セキュリティマネージャーISACAカンファランス in Tokyo
「デジタルトランスフォーメーション」時代におけるサイバーセキュリティ

坂　明
（一財）日本サイバー犯罪対策センターJC3 理事
（公財）東京オリンピック・パラリンピック競技大会CISO

JC3 Japan Cybercrime Control Center

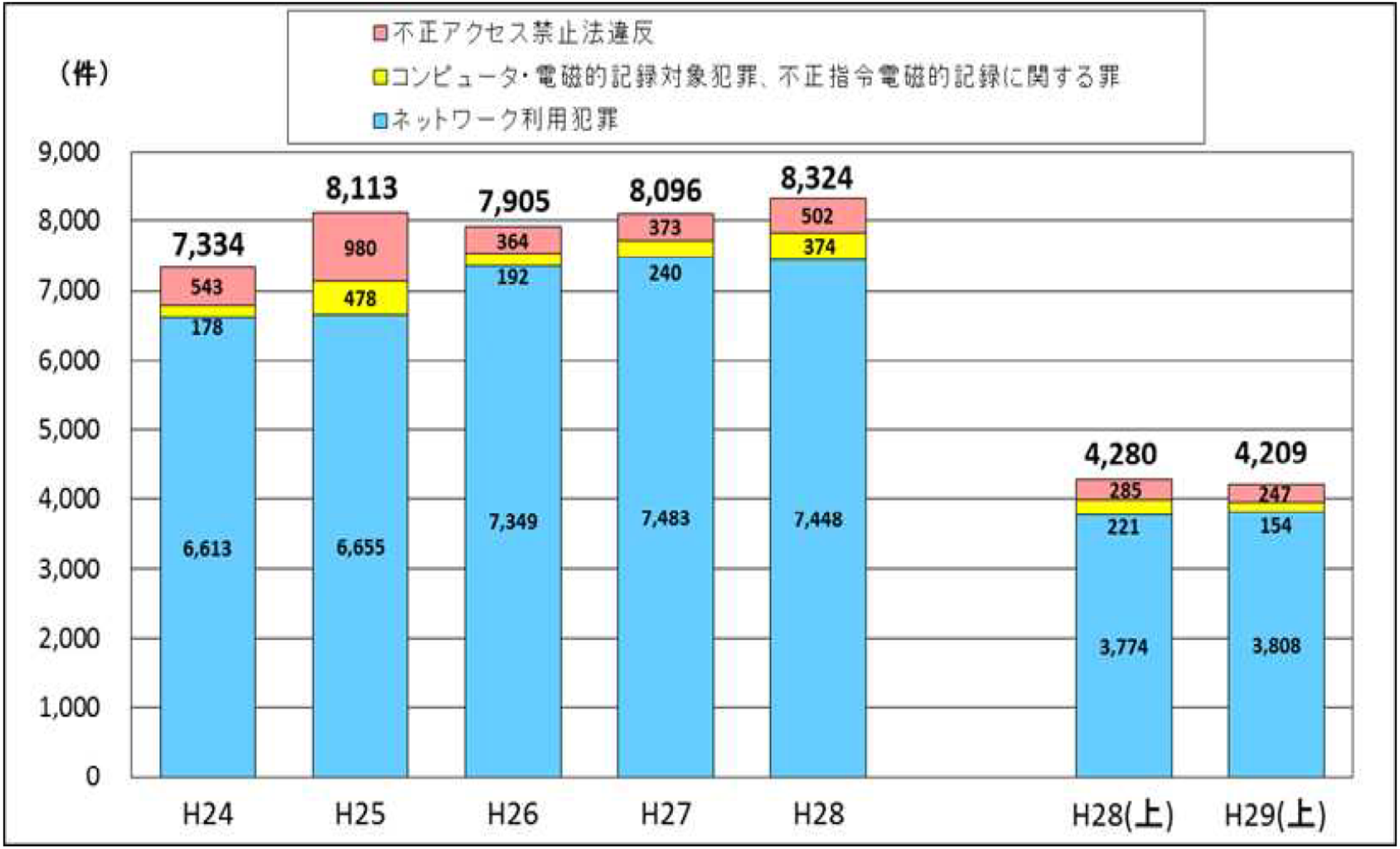
サイバー脅威の現状

本日の内容

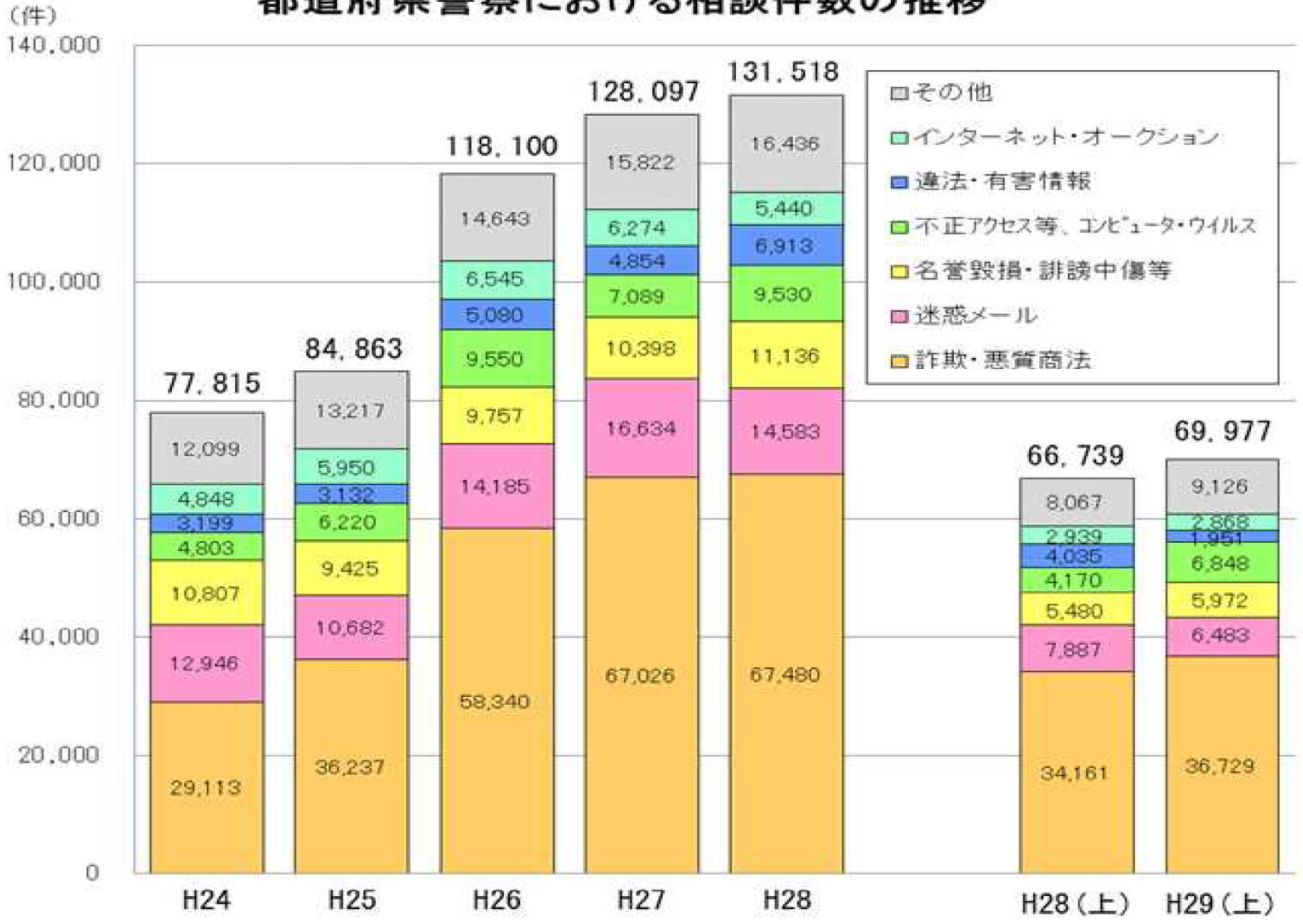
- **サイバー脅威の現状**
  - 概況
  - 金融犯罪の状況
  - eコマースをめぐる状況
- **JC3の活動**

サイバー犯罪の検挙件数

警察庁資料より



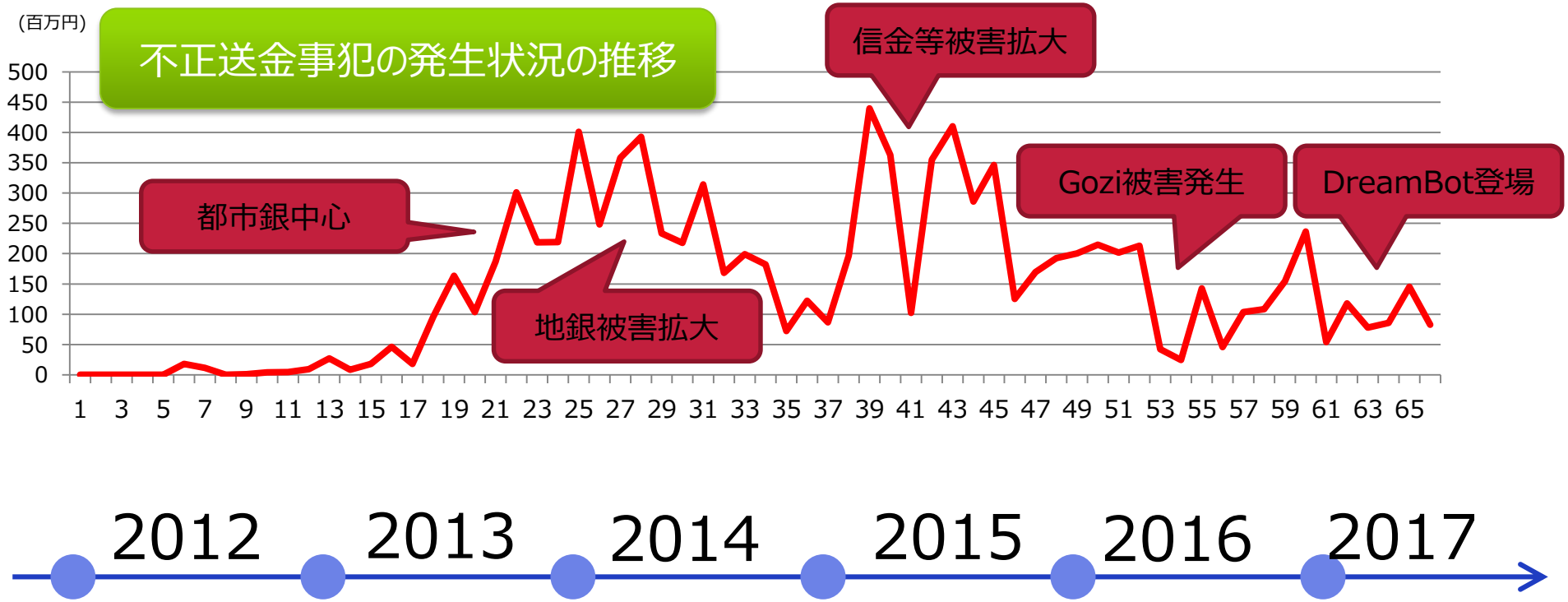
都道府県警察における相談件数の推移



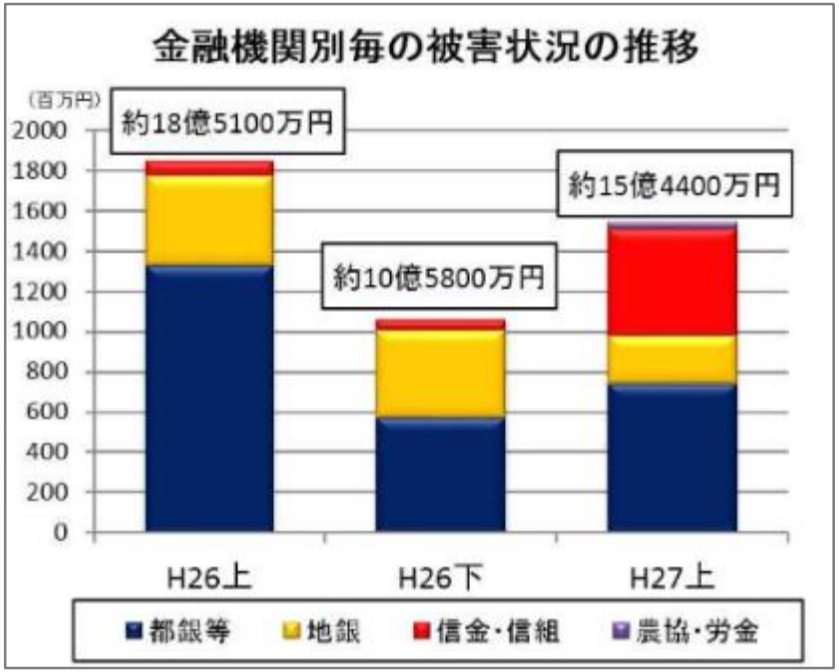
金融犯罪の状況

不正送金事案発生状況

H24	H25	H26	H27	H28
64件	1,315件	1,876件	1,495件	1,291件
約4,800万円	約14億600万円	約29億1,000万円	約30億7,300万円	約16億8,700万円



攻撃対象の推移（警察庁資料より）



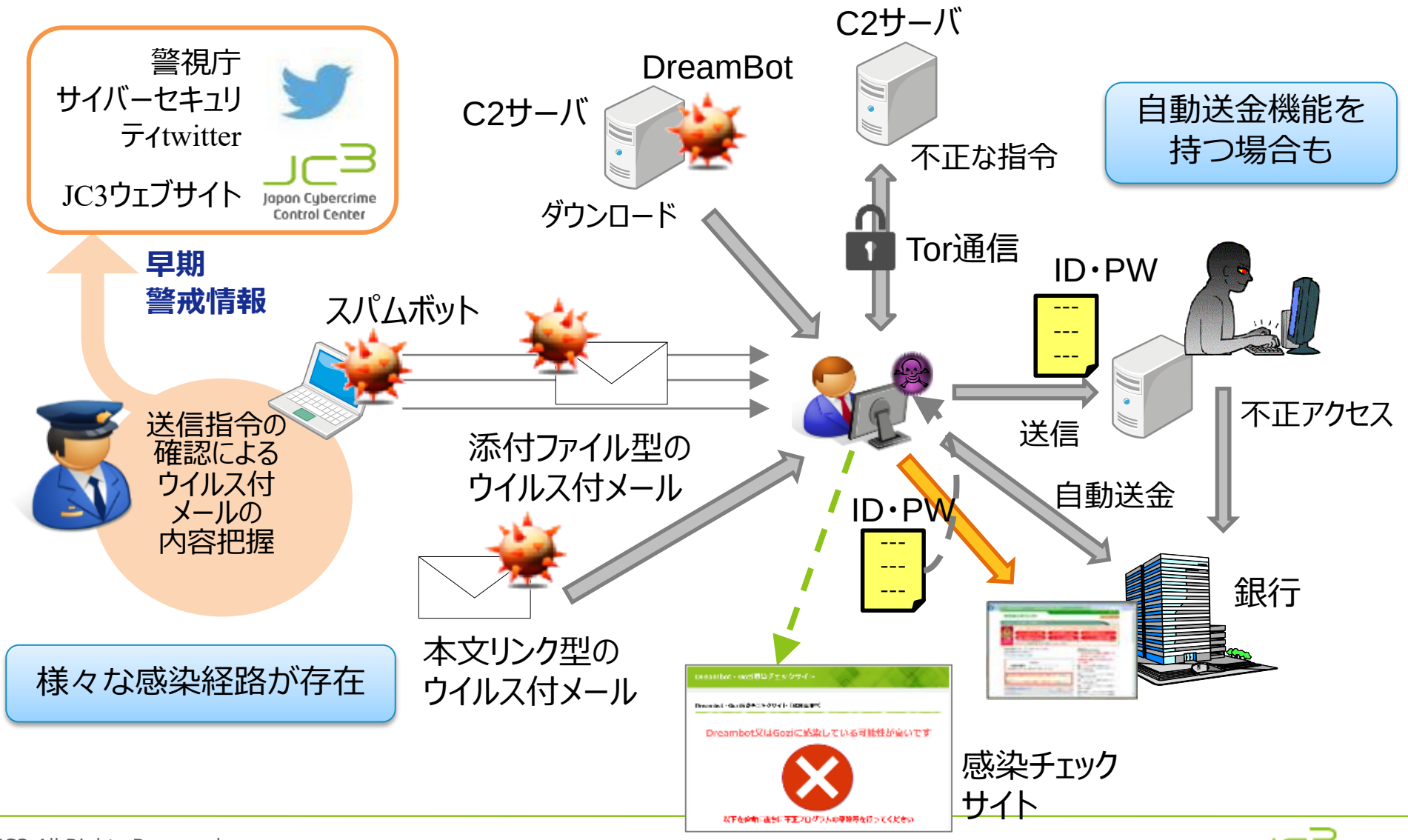
近時の不正送金手口の変遷

- **Gozi/DreamBotを使用した認証情報の窃取**
  - 窃取したアカウント情報を利用した銀行サーバへの不正アクセスによる不正送金の実施
    - いわゆる自動送金ウイルスも存在
  - 感染端末のリモートアクセスによる不正送金の実施
    - 電子証明書を利用している法人口座等
- **感染経路**
  - メール、誘導、水飲み場攻撃
- **送金先の変遷**
  - 中国人口座からベトナム人口座へ
  - ペイジー経由でギフトカード購入や仮想通貨購入
- **ワンタイムパスワードの窃取手法**
  - 電話によるOTPの聞き出し・入力手法の登場

サイバー脅威の現状と対応

- 目的を持った執拗な攻撃
  - 情報流出
  - 経済的利益
  - 特定の目的
- 組織的・有機的・自立的な攻撃
- 攻撃主体分析とそれを踏まえた対応
  - 脅威への対応のためには、脅威の分析が重要
  - サイバー攻撃（脅威）の発生メカニズムの把握
  - 武力攻撃、テロ、犯罪、示威行動等も含め目的の把握の重要性
  - 攻撃主体は人間であり、それを踏まえた対応

DreamBotへの感染につながるウイルス付メール



Cutwailによるウイルス付メール例

■昨年から続くウイルス付メール

【送信日】
2017年8月9日
【件名】
御請求書
【添付ファイル】
Doc_**0000000**.xls
【本文】
※次の2種類のいずれかになります

① お疲れ様です。
請求書が届き次第、お支払いについてお願いします

② お疲れ様です。
あなたはそれを8月14日までにお支払い下さい。

【送信日】
2017年8月9日
【件名】
写真
【添付ファイル】
IMG_Scan_**000**.xls
【本文】
お世話になっております
写真で
ご確認ください。
取り直しお願いします。

メール内容
請求書、写真、宅配業者、駐禁連絡…

Cutwailによる新たなウイルスメール例①

■2017年10月3日以降に検出

【送信日】
2017年10月6日
【件名】
【NTT-X Store】商品発送のお知らせ
【添付ファイル】

【本文】
注文番号X170516-**0000000**-0

◎本メールは発送時に、自動送信されております。

毎度ありがとうございます。「NTT-X Store」です。
ご注文頂いております商品を発送させていただきましたのでご報告申し上げます。
詳しくはこちら(※)

商品コード	EI1**0000000**
型番	SA5-271-F58U/F
商品名	SA5-271-F58U/F (i5/W10H64/H&Bprem/シルバー)
JANコード	451**0000000000**
出荷数	1
出荷日	2017/10/05
運送便	佐川急便EDI
送り状No	56**0000000000**

【送信日】
2017年10月12日
【件名】
【重要】カスタマセンターからのご案内【楽天カード株式会社】
【添付ファイル】

【本文】

【重要】カスタマセンターからのご案内

（ご注意：本メールにご返信頂くことはできません。）

平素は、楽天カードをご愛顧賜り誠にありがとうございます。
当社からの重要なご案内をお送りいたしますので、
下記内容をご確認いただきますよう、何卒お願い申し上げます。

□■---

■　振込先口座のご確認方法について

下記から楽天e-NAVIにログインいただき、ご確認いただけます。

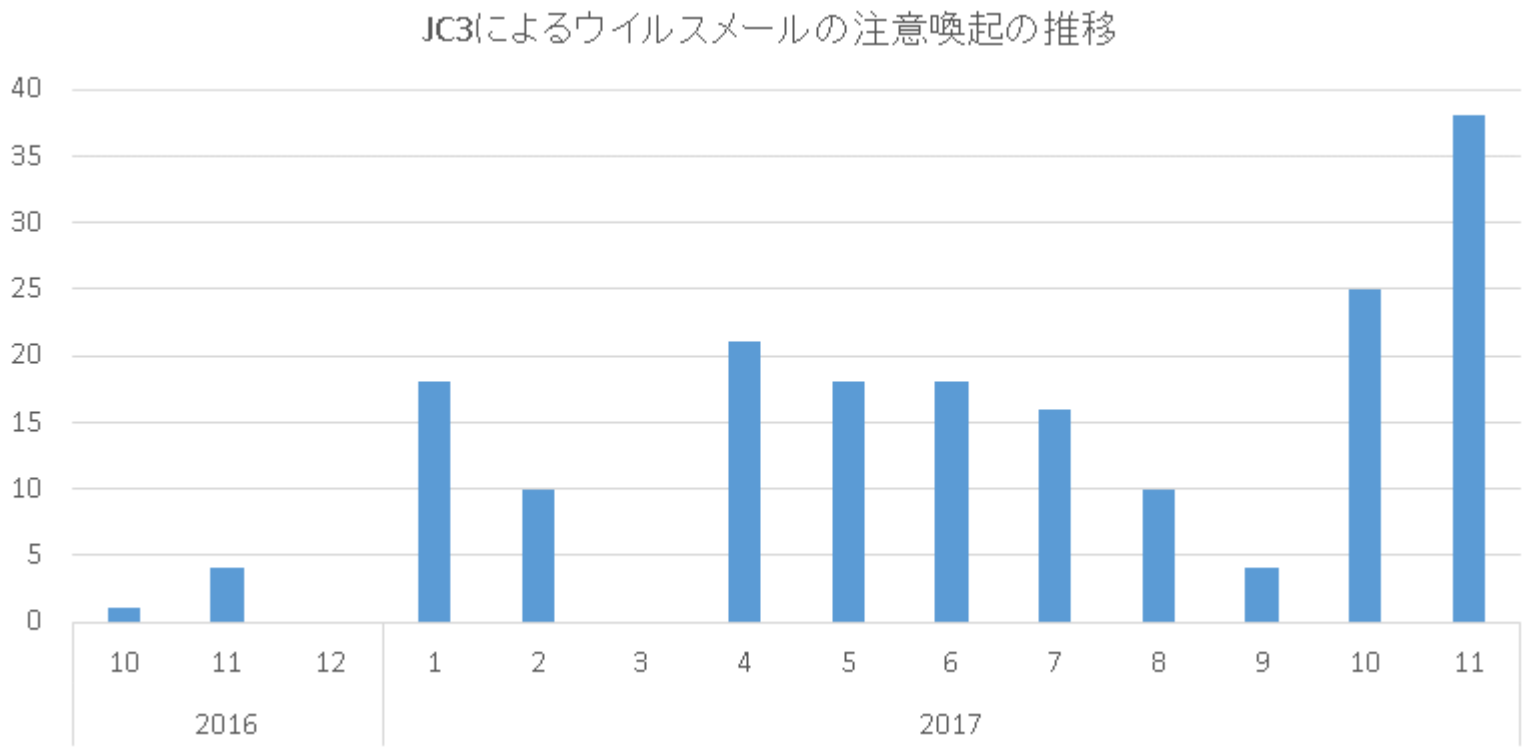
▼お客様への重要なお知らせ▼
詳しくはこちら(※)

メール内容
実在企業になりすましたリンク付きメール

メールシステムにおける
ウイルス対策を回避

ウイルス付メールの早期警戒情報の発信状況

- 平成28年11月より、警視庁と連携し、ウイルス付メールが配信される際に、件名や本文等を早期警戒情報として発信
- 平成29年11月末までに156件のウイルス付メールについて注意喚起
- 平成29年12月は、18日までで既に20件の注意喚起



中継サーバー事件関係（2014年11月）

- インターネット接続を中継する中継サーバ（プロキシサーバ）については、利用者のIPアドレスが置き換わるなどの特性を有しており、中継サーバを経由したサイバー犯罪の場合、その匿名性から被疑者特定に困難を極めている。
- 中継サーバ運営者の中には、不正アクセス行為等のサイバー犯罪に悪用されていると認識しながらサーボスを提供している悪質な運営者が存在している。
- これらを踏まえ、全国一斉で中継サーバ運営者等を検挙。

不正送金事犯捜査から割り出されたレンタルサーバ情報の提供

- 平成29年3月警察庁発表「平成28年中におけるサイバー空間における脅威の情勢等について」より

- 不正送金事犯で不正アクセスに利用されたレンタルサーバからのアクセスを遮断するため、28年４月、レンタルサーバのIPアドレスを警察庁から全国都道府県警察及び一般財団法人日本サイバー犯罪対策センター（ＪＣ３）を通じて金融機関に情報提供した。

December 5, 2016

Joint Cyber Operation Takes Down Avalanche Criminal Network

Servers Enabled Nefarious Activity Worldwide

It was a highly secure infrastructure of servers that allegedly offered cyber criminals an unfettered platform from which to conduct malware campaigns and "money mule" money laundering schemes, targeting victims in the U.S. and around the world.

国際的なサイバー犯罪インフラのテイクダウン作戦（Op.Avalanche）

警察によるインターネットバンキング利用者等への注意喚起

2017年3月23日

1. 警察による注意喚起

警察では、昨年実施された国際的なサイバー犯罪インフラのテイクダウン作戦（Op.Avalanche）に関連し、窃取されたとみられるインターネットバンキング利用者情報やインターネットバンキングマルウェアに感染している端末情報等を入手しており、関係する金融機関やインターネットサービスプロバイダ等と協力して利用者への注意喚起を実施しています。

注意喚起の連絡を受けた方は、インターネットバンキングの不正送金などのサイバー犯罪被害にあわないよう、警察庁からの注意喚起などを参考に、**マルウェアの感染について確認**を行うとともに、インターネットバンキングの**パスワード変更**を実施するなど、適切なセキュリティ対策を講じてください（警察庁からの注意喚起はこちら）。

なお、インターネットバンキングマルウェアDreambot・Goziについては、JC3で試験運用している**Dreambot・Gozi感染チェックサイト**もご活用ください（チェックサイトはこちら）。

2. 作戦概要

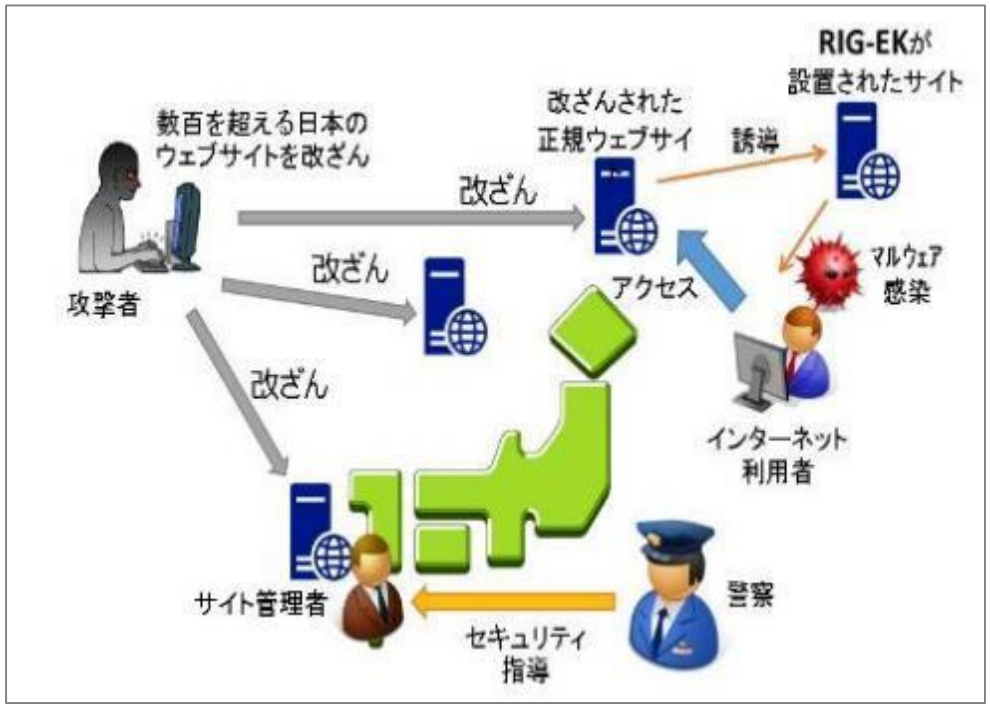
昨年、ドイツ警察を中心とした世界の法執行機関が連携し、インターネットバンキングの不正送金事犯の実行者を検挙するとともに、犯罪に利用された攻撃指令サーバ等の犯罪インフラを解体する国際的なテイクダウン作戦（Op.Avalanche）が実施されました。

3. 被害防止の取組

警察では、ドイツから提供された攻撃指令サーバに関する情報を分析し、窃取されたとみられるインターネットバンキング利用者のID・パスワード等の情報を確認したことから、関係する金融機関等に情報提供し、利用者への注意喚起を実施しています。

また、ドイツからマルウェアに感染しているとみられる端末の情報が提供されたことから、インターネットサービスプロバイダ等を通じ、感染端末の利用者に対してマルウェアの駆除を促す取組を実施しています。

改ざんサイト無害化の取組み

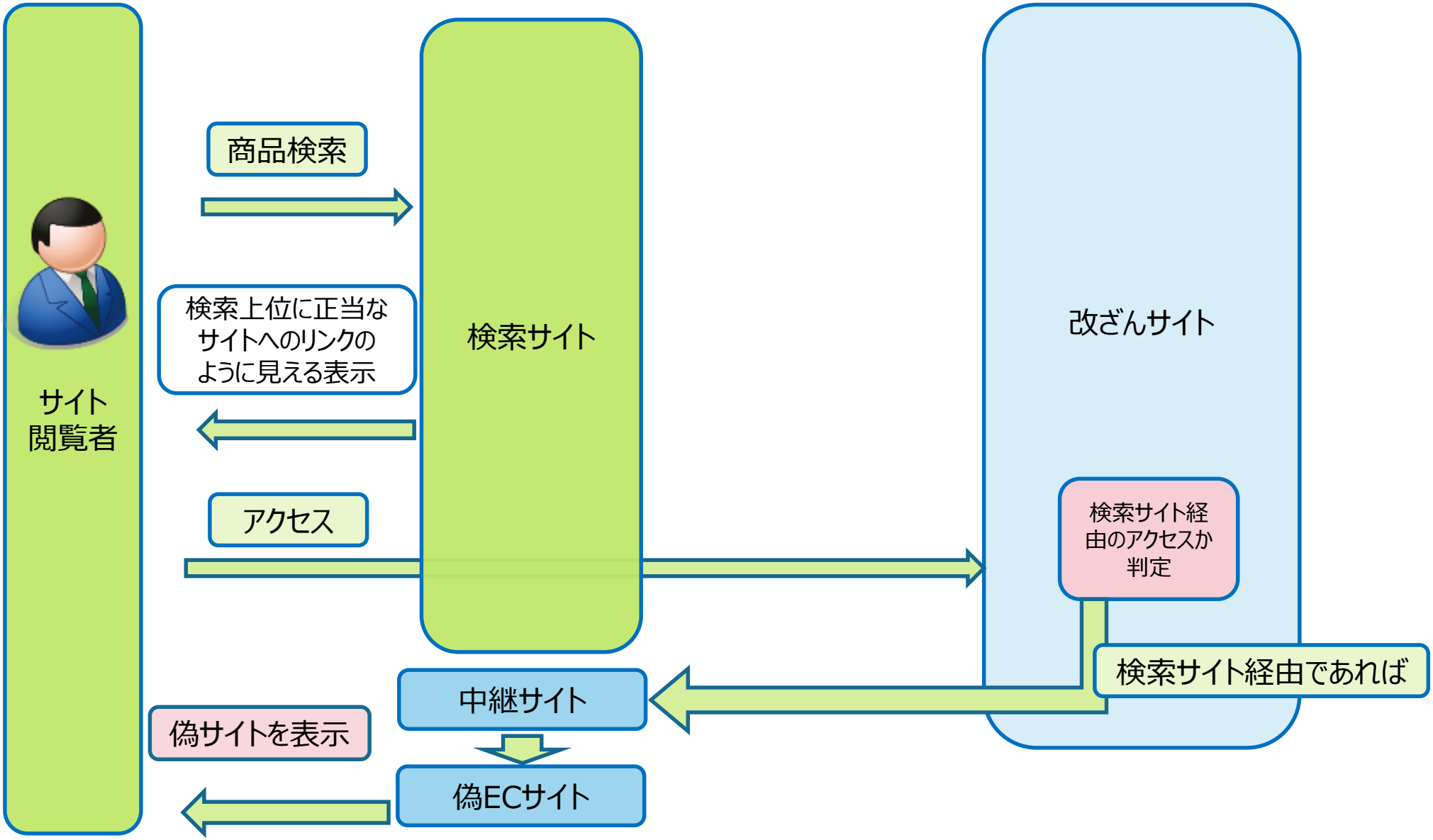


※Exploit Kit とは、アクセスした端末が保有する脆弱性に合わせ、端末にマルウェアを感染させることができるよう様々なプログラムをパッケージ化した攻撃ツール。

- ＪＣ３と会員企業の調査によって、「Rig Exploit Kit」（RIG-EK）が設置されたサイトに閲覧者を誘導するよう、日本のウェブサイトが多数改ざんされている事実を把握。
- 当該サイトにアクセスした場合、RIG-EKによって不正送金関連マルウェアやランサムウェアに感染する可能性があることが判明。
- ＪＣ３は、会員企業と協力し、改ざん手法の全容解明と全国の改ざんサイトの実態把握に着手。
- 各都道府県警察とも協力し、３８都道府県で２９８の改ざんウェブサイトの管理者に対し、改ざんされたサイトの修復や再発防止等に係るセキュリティ指導を実施。

eコマース対策

悪質サイト



悪質サイト対策

JC3等による広報など

詐欺サイト等悪質なショッピングサイトに関する注意喚起

2017年12月21日

JC3では、詐欺サイトやフィッシングサイト等の悪質なショッピングサイトによる被害を軽減するため各種取り組みを実施しております。

これら悪質サイトの多くは、インターネット利用者が**商品を検索した際に上位に表示されるように細工**されており、その**リンクを押下した利用者は悪質サイトに自動的に転送されます**。

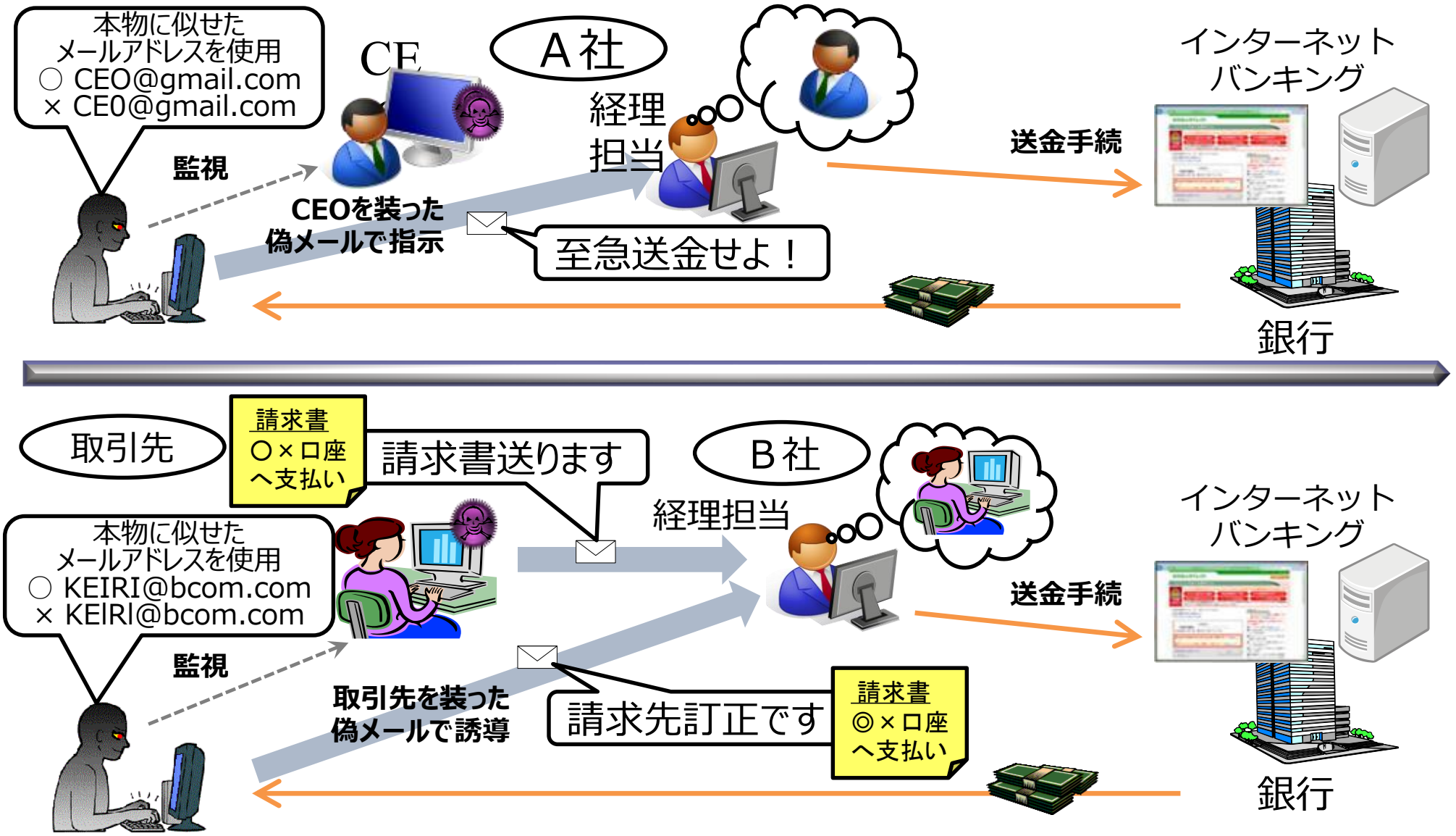
これらの悪質サイトには、代金を支払っても**商品を発送しなかったり**、会員登録時の**個人情報や決済時のクレジットカード情報等を盗み取ったりするサイトがあります**。

このためJC3では、警察庁、会員企業、APWG(※)と連携して、被害軽減のための情報提供と全容解明を図っています。

インターネット利用者は、このような被害を防止するため市販のセキュリティ対策ソフト・フィルタリングソフトを導入し、基本ソフト（OS）やウェブブラウザーなどの各ソフトウェアを常に最新の状態に更新にするとともに、オンラインショッピングをする際は下記の点に注意するなど被害防止対策を行って下さい。

（※）APWG(Anti Phishing Working Group)： 米国に本拠を置く世界最大のフィッシング対策の国際機関

法人メール詐欺（Business Email Compromise）



よくみられるBECの手法

- **メールアカウントを悪用される対象**
  - 役員、上級管理職
  - 取引先
  - 一般職員
- **メールアカウントを乗っ取る手法**
  - フィッシング
  - 標的型攻撃
  - マルウェア
- **メールを用いた欺罔行為**
- **類似ドメインを登録して悪用**

JC3の活動

JC3の概要

- **法人名　　一般財団法人 日本サイバー犯罪対策センター**
  （英語名：Japan Cybercrime Control Center　略称：JC3）
- **業務開始日　平成26年11月13日**
- **目的**
  サイバー空間全体を俯瞰し、産学官(警察)それぞれが持つサイバー空間の脅威への対処経験を集約・分析した情報を組織内外で共有し、サイバー空間の脅威を特定、軽減及び無効化するための活動に貢献する。
- **事業内容**
  - サイバー空間の脅威に関する情報の集約・分析
  - 研究・人材育成
  - 国際連携
- **米国NCFTA（JC3のモデル）の基本ポリシー**
  - “One team, one goal”
  - “F2F（Face to Face）”（直接会って）
  - “Industry First”（「民間を第一に」）
  - “Focus on what you can share and are comfortable sharing”（共有できる情報、共有しても支障のない情報にフォーカスしよう）

米国NCFTAとは

NCFTA = National Cyber-Forensics & Training Alliance

サイバー空間の脅威の深化

↓

法執行機関・民間企業・学術団体の連携による効果的対応の必要性

↓

NCFTAの設立

設立

平成9年設立
（米国ピッツバーグ）

組織

法執行機関・民間企業・学術団体を構成員とする非営利団体

目的

産学官における情報共有と協力の促進によるサイバー空間の脅威の効率的な特定、軽減及び無効化

機能

- サイバー犯罪に係る情報の集約と分析
- トレーニングの提供
（諸外国の捜査機関の捜査員が参加）　等

設立の背景　～日本における検討の経緯～

以下のような政府の枠組み等において、日本版ＮＣＦＴＡの創設を検討

- サイバーセキュリティ戦略

  （平成25年6月10日　情報セキュリティ政策会議）

- サイバーセキュリティ2013

  （平成25年6月27日　情報セキュリティ政策会議）

- 「世界一安全な日本」創造戦略

  （平成25年12月10日　閣議決定）

- 平成25年度総合セキュリティ対策会議報告書

  （平成26年1月30日　総合セキュリティ対策会議）

- サイバーセキュリティ2014

  （平成26年7月10日　情報セキュリティ政策会議）

JC3 御賛同いただいている企業・機関

1. 株式会社エヌ・ティ・ティ・データ
2. 株式会社KPMG FAS
3. 株式会社ジェイティービー
4. セコム株式会社
5. 株式会社ソリトンシステムズ
6. デロイト トーマツ リスクサービス株式会社
7. トレンドマイクロ株式会社
8. 日本アイ・ビー・エム株式会社
9. 日本電気株式会社
10. 株式会社日立製作所
11. 富士通株式会社
12. 株式会社みずほ銀行
13. 株式会社三井住友銀行
14. 株式会社三菱東京ＵＦＪ銀行
15. ヤフー株式会社
16. 株式会社ゆうちょ銀行
17. 株式会社ラック

- 情報セキュリティ大学院大学、首都大学東京、東京電機大学
- 警察庁

1. EASY SOLUTIONS JAPAN合同会社
2. 株式会社インフォセック
3. Ｓ＆Ｊ株式会社
4. NRIセキュアテクノロジーズ株式会社
5. 株式会社ＦＦＲＩ
6. 株式会社サイバーディフェンス研究所
7. サン電子株式会社
8. シスコシステムズ合同会社
9. 株式会社シマンテック
10. 全日本空輸株式会社
11. 綜合警備保障株式会社
12. 東京海上日動火災保険株式会社
13. ネットワンシステムズ株式会社
14. バングガード株式会社
15. PwCサイバーサービス合同会社
16. ファイア・アイ株式会社
17. フォーティネットジャパン株式会社
18. マカフィー株式会社
19. 株式会社三越伊勢丹システム・ソリューションズ
20. 楽天株式会社
21. ラストライン合同会社
22. 株式会社リクルートホールディングス　(敬称略)

JC3 評議員・理事・監事

評議員　（50音順、敬称略）

- 片桐 裕
  (公財)公共政策調査会理事長(元警察庁長官)
- 隅 修三
  東京海上ホールディングス（株）取締役会長
- 田尾 健二郎
  元広島高等裁判所長官,元国家公安委員会委員
- 林 紘一郎
  情報セキュリティ大学院大学　教授
- 前田 雅英
  日本大学大学院　法務研究科教授

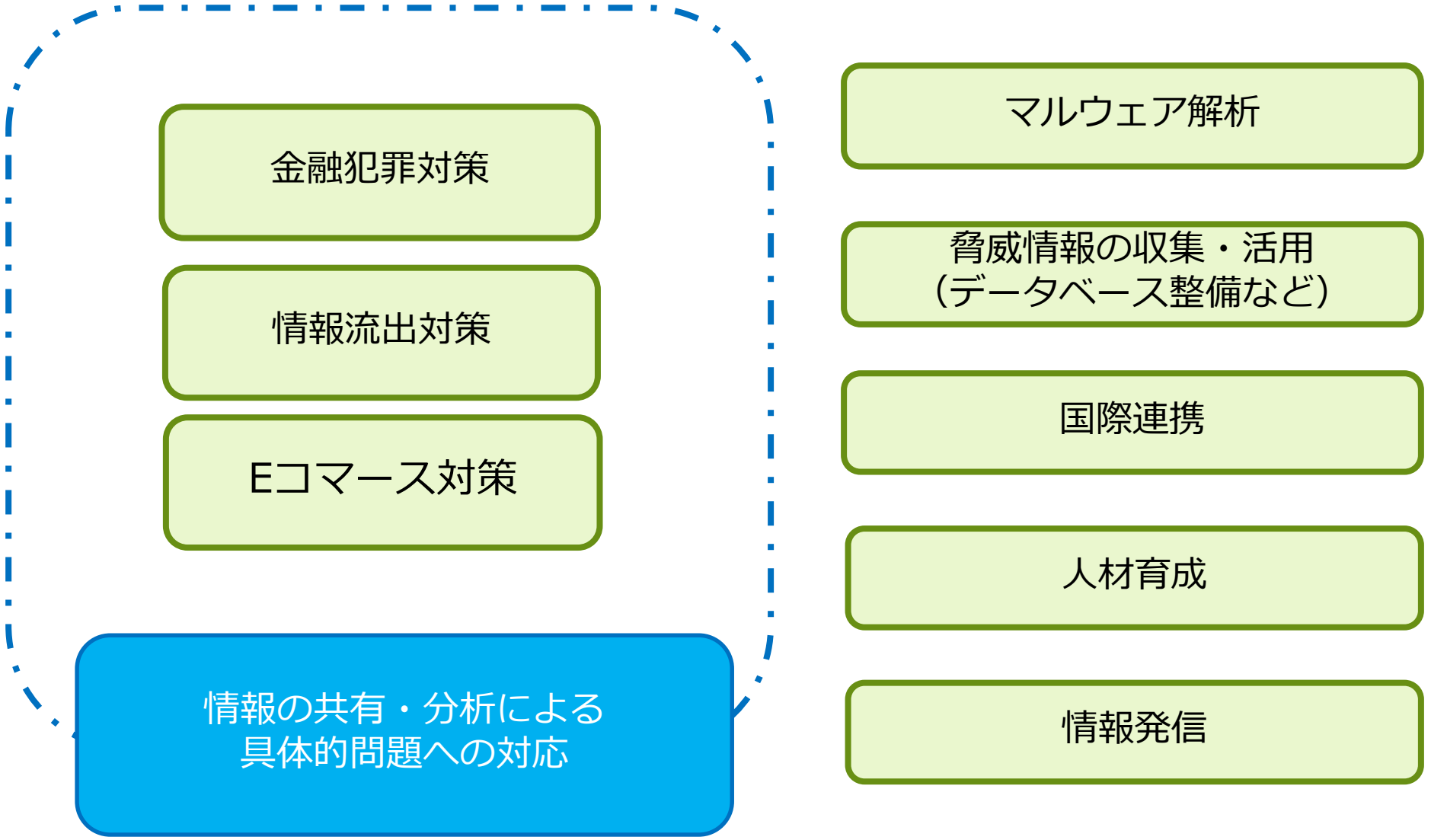
監事　（敬称略）

- 宮下　正彦　　弁護士

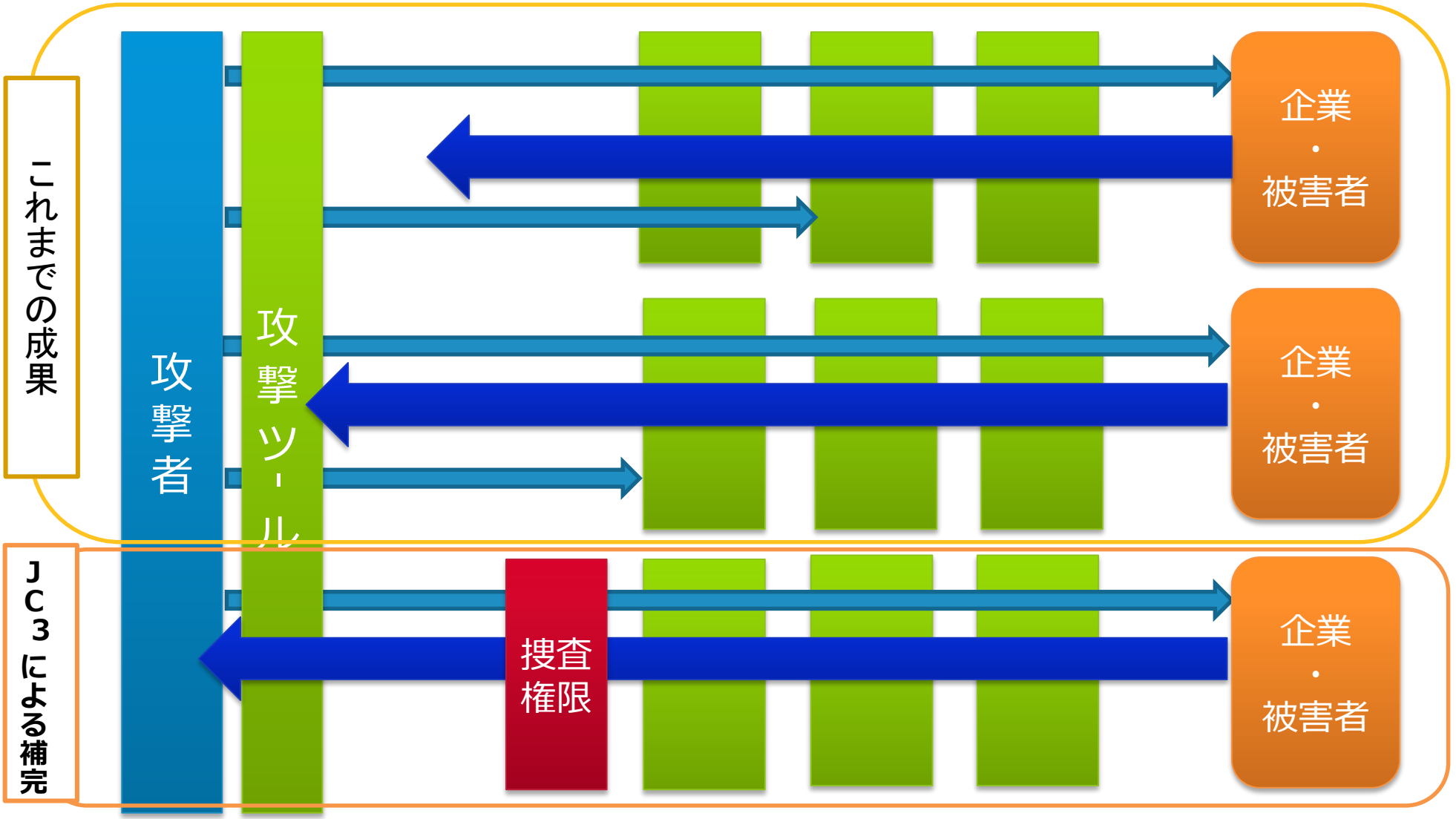
理事　（50音順、敬称略）

1. 相川 浩啓　　株式会社みずほ銀行
2. 岩井 博樹
   デロイト トーマツ リスクサービス株式会社
3. 岡田 昭宏　富士通株式会社
4. 尾崎 寛　　株式会社三井住友銀行
5. 坂 明　　JC3常勤
6. 清水 智　　トレンドマイクロ株式会社
7. 清水 隆明　　日本電気株式会社
8. 西本 逸郎　　株式会社ラック
9. 藤川 春久　　セコム株式会社
10. 別所 直哉　ヤフー株式会社
11. 星 周一郎　　首都大学東京
12. 松野 善方　　株式会社三菱東京UFJ銀行
13. 安田 浩　　東京電機大学
14. 遊佐 洋　　株式会社ソリトンシステムズ

JC3の活動内容



JC3の役割



情報発信活動について

1. フォーラム

- 毎年、サイバーセキュリティ月間となる２月１日から３月１８日までの間を目途にフォーラムを開催し、広く社会に対し、サイバー脅威の状況やJC3の活動内容などの情報共有を行っている。
- JC3フォーラム2018は、2018年3月13日（火）に開催予定

2. ワークショップ

- 年に２回程度、全会員及び信頼関係を構築できると見込まれる者等との情報共有の場として、ワークショップを開催し、より具体的なサイバー脅威の状況やJC3の活動内容などの情報共有を行っている。

情報発信活動について

3. ウェブサイト等での情報発信

- 活動内容等について情報提供するウェブサイトを、適宜更新しつつ運営している。また、活動により得られた情報・知見のうち、注意喚起情報等一般に提供することが有益と考えられるものは、情報提供者の意向を踏まえた上で掲載している。
- また、JC3の活動トピック概要を纏めた「ニューズレター」を隔月程度の間隔で全会員向け発信している。
- 会員及び連携団体に向けて、JC3ウェブサイトを更新した際や重要なお知らせがある時等に、適宜その旨を情報発信するメール配信も実施している。

4. 関係機関等への情報提供

- 都道府県警察を含む警察機関やその他関係機関に対して、また各種セキュリティ関連イベント等において、JC3の活動内容について情報提供し、JC3の活動をアピールすると共に協働への働きかけを行っている。

JC3の活動の展開

- **脅威の実態解明に資する情報共有・分析ー新たな課題への取組み**
  - 深い情報共有・分析による脅威の全体像の把握と対策の検討（現時点において対応上問題となっているポイントの把握も含む）
- **JC3の環境を活用した脅威の特定・軽減・無効化活動の展開**
  - 法執行機関との連携
- **具体的な脅威の特定・軽減・無効化活動に資する情報共有等**
  - 情報の共有・分析やJC3プラットフォームを活用した対応の展開
- **協働による能力の向上**
- **NCFTAをはじめとする海外連携による活動の展開**
- **さまざまな問題事象の相談対応**
  - 新たな課題となり得る問題事象について、官民で連携して対応
- **情報共有組織との連携**
- **さまざまな組織との連携**
- **東京オリンピック・パラリンピック競技大会に向けた取組み**


JC3
Japan Cybercrime Control Center