

第5回情報セキュリティマネージャー
ISACA カンファレンスin Tokyo

金融機関におけるサイバーセキュリティ 管理態勢整備の現状と課題

2017年2月18日



Building a better
working world



Contents

1. 金融機関とサイバーセキュリティ
2. 金融機関のサイバーセキュリティへの取組み
3. サイバーセキュリティ管理態勢の整備に向けて


※本講演資料は、組織を代表してのものではなく、現時点での私の個人的な考えを述べたものです。

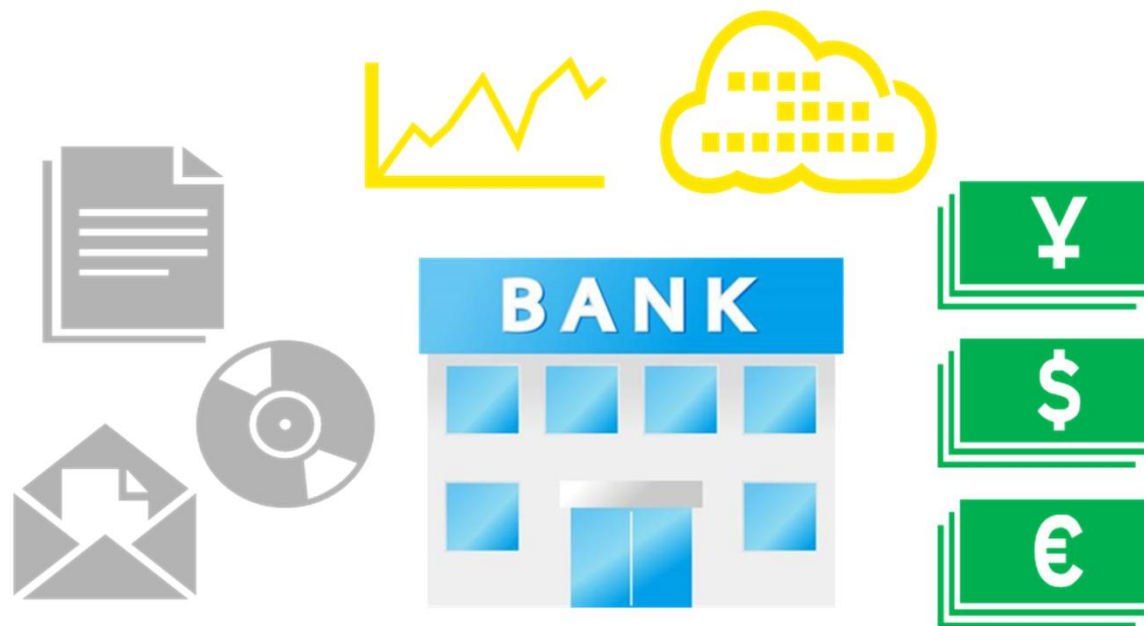
※本公演資料の中でお話する事例は、個別の特定クライアントに係る話ではありません。



1. 金融機関とサイバーセキュリティ

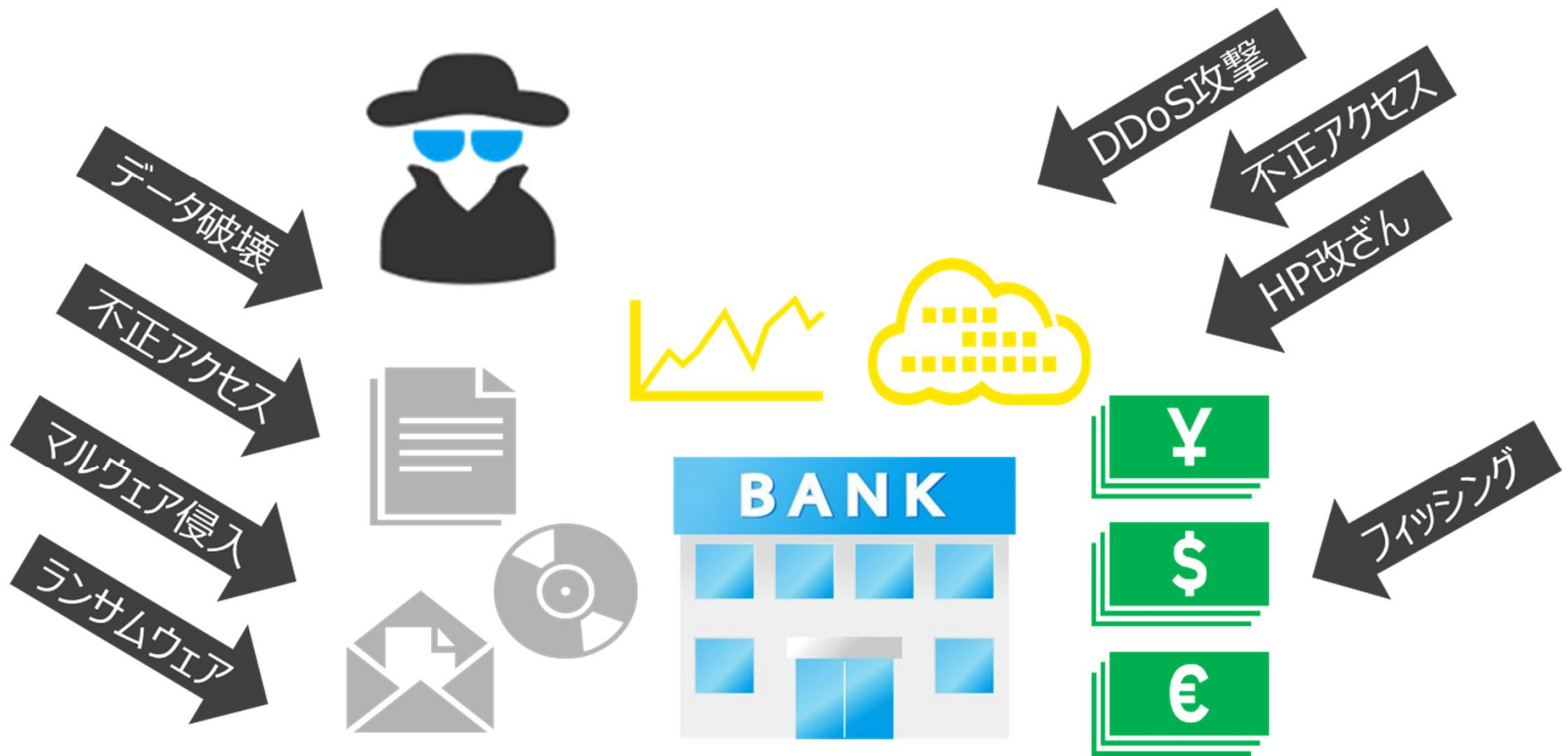
金融機関

- ▶ 金融取引に関する業務を営む組織
- ▶ 都市銀行、地方銀行、信託銀行、信用金庫、信用組合、農業協同組合、漁業協同組合、保険会社、証券会社、ノンバンク、などなど
- ▶ お金と情報を持っている ←だから狙われる 



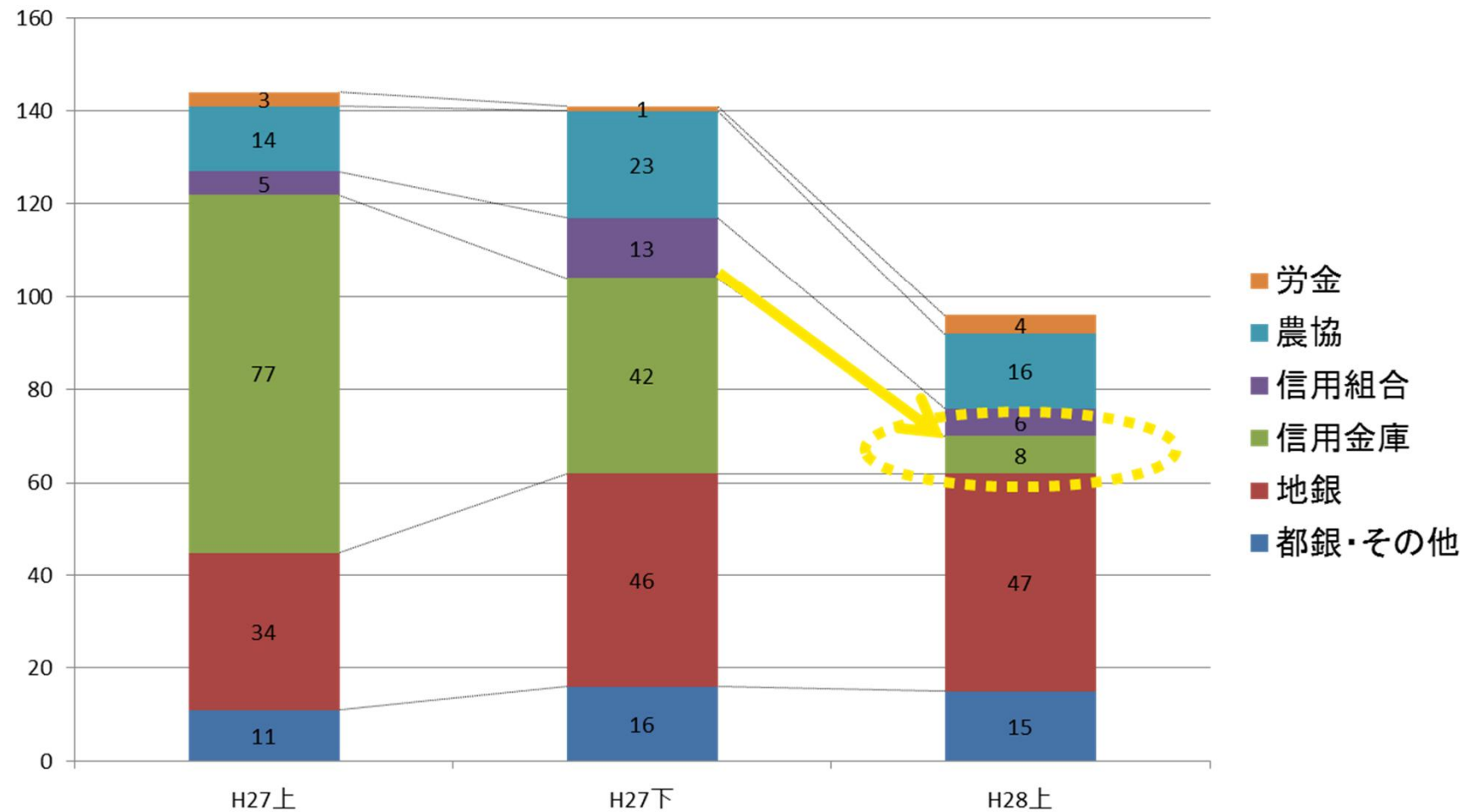
金融機関へのサイバー攻撃ベクトル

- ▶ 直接的に金銭を狙う攻撃、情報窃取(顧客情報・機密情報等)、妨害行為等々いろいろ



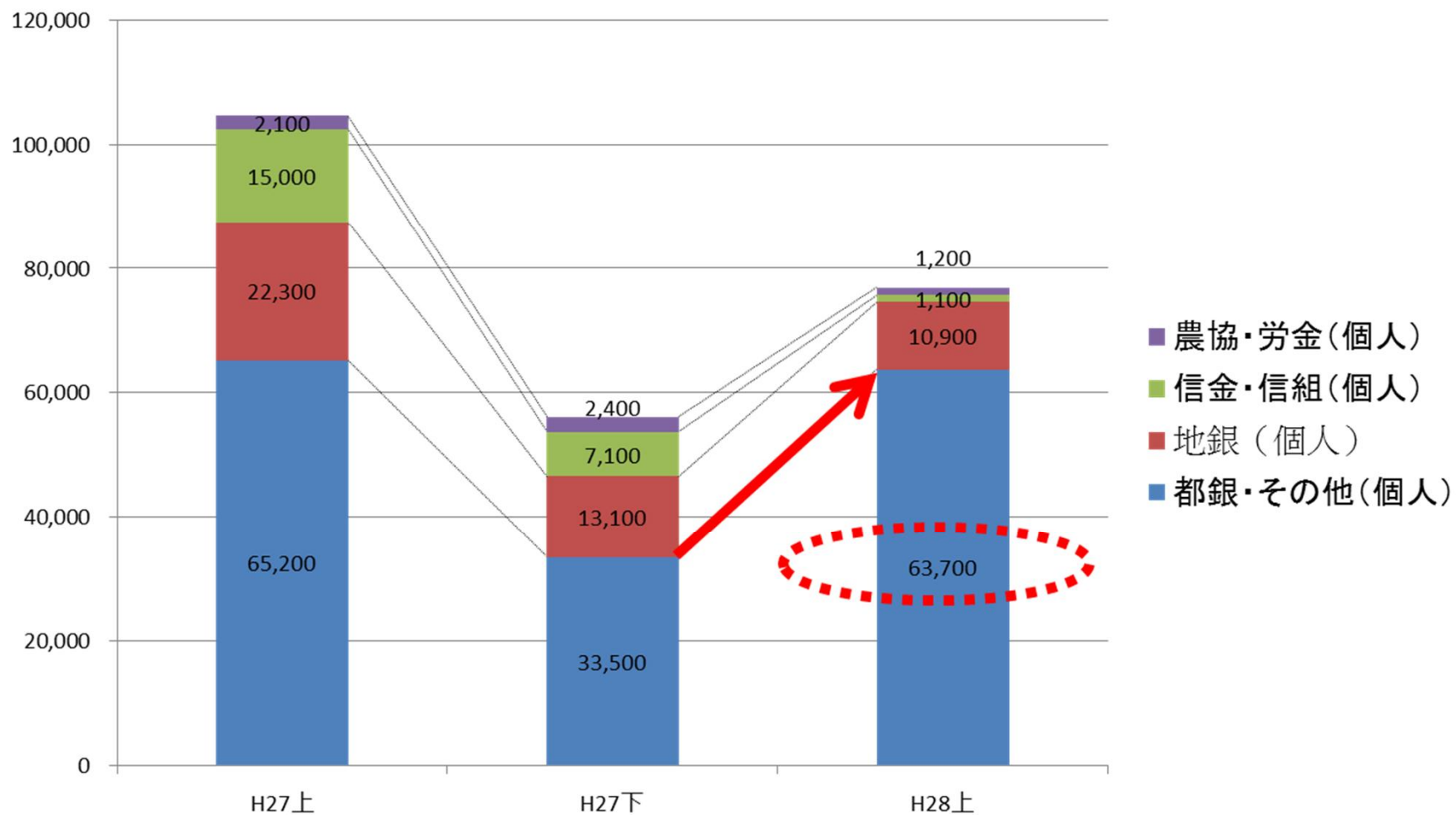
2016上半期インターネットバンキングに係る不正送金事犯の状況

被害金融機関数の推移



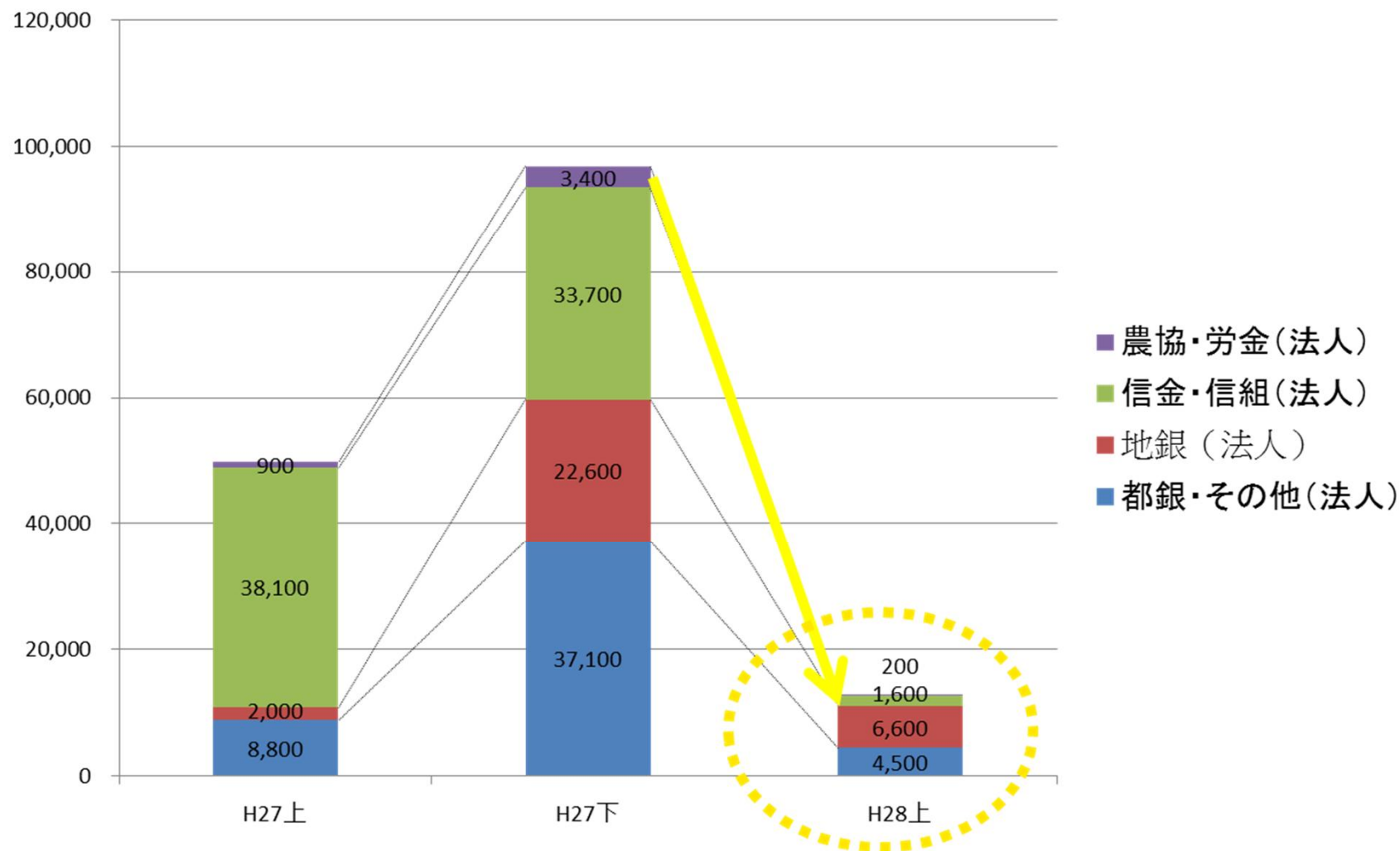
2016上半期インターネットバンキングに係る不正送金事犯の状況

金融機関別被害金額の推移(個人口座)



2016上半期インターネットバンキングに係る不正送金事犯の状況

金融機関別被害金額の推移(法人口座)



金融機関とサイバーセキュリティ規制

- ▶ 金融業は金融庁の免許・許可事業であり、金融庁の金融行政の下で事業を行っている。

**金融庁**
Financial Services Agency

[広報報道](#) | [利用者の方へ](#) | [金融庁について](#) | [金融機関情報](#)

[ホーム](#) >

法令・指針等

金融検査マニュアル関係

- ・  [預金等受入金融機関に係る検査マニュアル\(PDF:5,257KB\)](#) 項目別
 - ▽  [金融検査マニュアルに関するよくあるご質問\(FAQ\)\(PDF:1,219KB\)](#)
 - ▽  [金融検査マニュアルに関するよくあるご質問\(FAQ\)別編《ABL編》\(PDF:202KB\)](#)
- ・  [金融検査マニュアル別冊〔中小企業融資編〕 項目別](#)

監督指針・事務ガイドライン

監督指針

- ・ 主要行等向けの総合的な監督指針
 - 本文([HTML版](#)・ [PDF版\(4,456KB\)](#)) [様式・参考資料編](#)
 - 英語版(外国銀行支店関連箇所)( [PDF版\(153KB\)](#))
- 平成23年東北地方太平洋沖地震による災害に関する主要行等向けの総合的な監督指針の特例措置について([HTML版](#)・ [PDF版\(21KB\)](#))

金融庁HPより引用

金融機関とサイバーセキュリティ規制

- ▶ 「サイバー攻撃は**金融システム全体に対する最大の脅威の一つ**」

平成28事務年度 金融行政方針

主なポイント



平成28年10月
金融庁

IT技術の進展による金融業・市場の変革への戦略的な対応

FinTechへの対応

FinTech(金融・IT融合)の動きが、**金融の姿を今後大きく変えていく**ことが見込まれる

サービスの**イノベーション**を通じて、国民にとってより良いサービスの提供が図られるよう、必要と
制度面の**対応について機動的に検討**するとともに、**決済インフラの高度化、新たな金融技術の活
推進**

既存の金融機関は、組織・人材・システム等の見直しも含め、**変革に向けた果敢な意思決定を遅滞な
く行う必要があり、我が国金融機関のタイムリーな対応を促進**

▶ **FinTechベンチャーの登場・成長が進んでいく環境の形成**に向けた取組みを継続

(2) サイバーセキュリティの強化

- ▶ サイバー攻撃は**金融システム全体に対する最大の脅威の一つ**
- ▶ 金融分野のサイバーセキュリティの底上げを図るため、初の**金融業界横断的な演習**を実施

(3) アルゴリズム取引等への対応

- ▶ アルゴリズムを用いた高速な取引について、**欧米における規制等の動向も踏まえ、対応を検討**

金融庁HPより引用

「重要インフラ事業者」としての金融機関

セプター特性把握マップ

重要インフラ分野	情報通信			金融				航空	鉄道	電力
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	鉄道	電力
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	航空分野におけるCEPTOAR	鉄道CEPTOAR	電力CEPTOAR
事務局	(一社) ICT-ISAC	(一社) 日本ケーブルテレビ連盟	(一社) 日本民間放送連盟	(一社) 全国銀行協会 事務・決裁システム部	日本証券業協会 IT統括部	(一社) 生命保険協会 総務部組織法務グループ	(一社) 日本損害保険協会 IT推進部品質グループ	定期航空協会	(一社) 日本鉄道電気技術協会	電気事連合会 情報通信部
構成員(内訳)	24社・団体 (固定系のネットワークを構築する電気通信事業者、IPネットワークの電気通信事業者、ISP事業者、携帯電話事業者等)	332社 (一社)日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者)	194社・1団体 (日本放送協会、地上系民間放送事業者、(一社)日本民間放送連盟)	1,433社 (銀行、信用金庫、信用組合、労働金庫、農協等)	260社・7機関 (金融商品取引業者、取引所等証券関係機関)	41社 (一社)生命保険協会の定款に定める社員および特別会員)	29社(オブザーバ3社含む) (一社)日本損害保険協会 情報システム委員会 参加会社)	14社・1団体 (航空運送事業者、定期航空協会)	22社・1団体 (鉄道事業者22社、1団体)	12社・2機関 (一般電気事業者、本原電(株)、電事連合会電力中央研究所)
緊急窓口	2007年4月運用開始	2012年12月運用開始		2007年4月運用開始						
情報の取扱ルール	2007年1月制定	2012年11月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2006年9月制定
連絡手段	メール	メール 電話	メール 電話	メール WEB	メール WEB	メール 電話 FAX 携帯電話	メール WEB	メール	メール	メール 携帯電話

金融			
銀行等	証券	生命保険	損害保険
金融CEPTOAR連絡協議会			
銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR
(一社) 全国銀行協会 事務・決裁システム部	日本証券業協会 IT統括部	(一社) 生命保険協会 総務部組織法務グループ	(一社) 日本損害保険協会 IT推進部品質グループ
1,433社	260社 7機関	41社	29社 (オブザーバ3社含む)
(銀行、信用金庫、信用組合、労働金庫、農協等)	(金融商品取引業者、取引所等証券関係機関)	((一社)生命保険協会の定款に定める社員および特別会員)	((一社)日本損害保険協会 情報システム委員会 参加会社)

http://www.nisc.go.jp/active/infra/pdf/cc_ceptoar.pdf

「重要インフラ事業者」としての金融機関

- ▶ 2020オリパラを視野に、第3次行動計画の枠組みを維持しつつ、取組を強化・改善。

重要インフラの情報セキュリティ対策に係る 第4次行動計画（案）

パブコメ〆切：平成29年2月16日（木）17時

平成 年 月 日
サイバーセキュリティ戦略本部

Ⅱ. 本行動計画の要点	9
Ⅲ. 計画期間内に取り組む情報セキュリティ対策	11
1. 安全基準等の整備及び浸透	11
1.1 指針の継続的改善	11
1.2 安全基準等の継続的改善	12
1.3 安全基準等の浸透	12
2. 情報共有体制の強化	13
2.1 本行動計画期間における情報共有体制	13
2.2 情報共有の更なる推進	14
2.3 重要インフラ事業者等の活動の更なる活性化	15
3. 障害対応体制の強化	16
3.1 分野横断的演習の改善	16
3.2 セブター訓練	17
4. リスクマネジメント及び対処態勢の整備	18
4.1 リスクマネジメントの標準的な考え方	18
4.2 リスクマネジメントの推進	19
4.3 本施策と他施策による結果の相互反映プロセスの確立	22
5. 防護基盤の強化	23
5.1 重要インフラに係る防護範囲の見直し	23
5.2 広報広聴活動の推進	24
5.3 国際連携の推進	24
5.4 セキュリティ・バイ・デザインの推進	25
5.5 経営層への働きかけ	25
5.6 人材育成等の推進	26
5.7 マイナンバーに関するセキュリティ確保	26
5.8 規格・標準及び参照すべき規程類の整備	26

「重要インフラの情報セキュリティ対策に係る 第4次行動計画(案)」

- ▶ 重要インフラ防護に責任を有する**政府と**自主的な取組を進める**重要インフラ事業者等との共通の行動計画**。
- ▶ 重要インフラの防護にあたっては、サービス提供に必要な情報システムについて、サイバー攻撃等による障害の発生を**可能な限り減らす**とともに、障害発生時の**早期検知**や、障害の**迅速な復旧**を図ることが重要。
- ▶ 「**機能保証**」: 重要インフラサービスを安全かつ持続的に提供するための取組みで、各関係主体が重要インフラサービスの防護や機能維持を**確約することではなく**、各関係主体が重要インフラサービスの防護や機能維持のための**プロセスについて責任を持って請け合うことを意図**している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する**必要な努力を適切に払うことを求める**考え方。

重要インフラ事業者等(経営層)に求められる取組

- ▶ **経営層が積極的に関与**し、情報セキュリティに係るリスクへの備えを経営戦略として位置付け、リスクアセスメントの結果を踏まえた**リスク低減等の対応を戦略的に講じる**とともに、サイバー攻撃等に遭遇した場合であっても、重要インフラサービスの安全を確保し、かつ、自ら及びステークホルダーが許容できない停止・品質低下を可能な限り生じさせずに**重要インフラサービスの提供を継続**できるように、**適切な対処態勢を整備すること**などが求められる。また、経営層は、情報セキュリティ対策に係る**内部統制システム**を整備した上、こうした**機能保証のための取組が適切に講じられている**ことについて、自らのステークホルダーに対する**アカウンタビリティを果たす**ことが重要である。
- ▶ 機能保証の観点から適切な対処態勢を整備するためには、リスクマネジメントのプロセスにおけるリスクアセスメント、リスクコミュニケーション及び協議、モニタリング及びレビュー等の**取組を強化・推進**することが**求められる**。

重要インフラ事業者等の経営層の在り方ー①

- ▶ **経営層**は、以下の項目の必要性を認識し、**実践すること**。
- ▶ 自らの**状況を正しく認識**し、活動目標を**主体的に策定**するとともに、各々必要な取組の中で**定期的に**自らの対策・施策の**進捗状況を確認**する。また、他の関係主体の活動状況の把握に努め、相互に自主的に協力する。
- ▶ 重要インフラサービス障害の規模に応じて、**情報に基づく対応の5W1Hを理解**しており、重要インフラサービス**障害の予兆及び発生に対し冷静に対処ができる**。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携や統制の取れた対応ができる。
- ▶ **情報セキュリティの確保は経営層が果たすべき責任**であり、経営者自らがリーダーシップを発揮し、**機能保証の観点から情報セキュリティ対策に取り組むこと**。

重要インフラ事業者等の経営層の在り方②

- ▶ 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン(**ビジネスパートナーや子会社、関連会社**)を含めた**情報セキュリティ対策**に取り組むこと。
- ▶ 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する**情報の開示等**に取り組むこと。
- ▶ 上記の各取組に必要な予算・体制・人材等の**経営資源を継続的に確保**し、リスクベースの考え方により**適切に配分**すること。

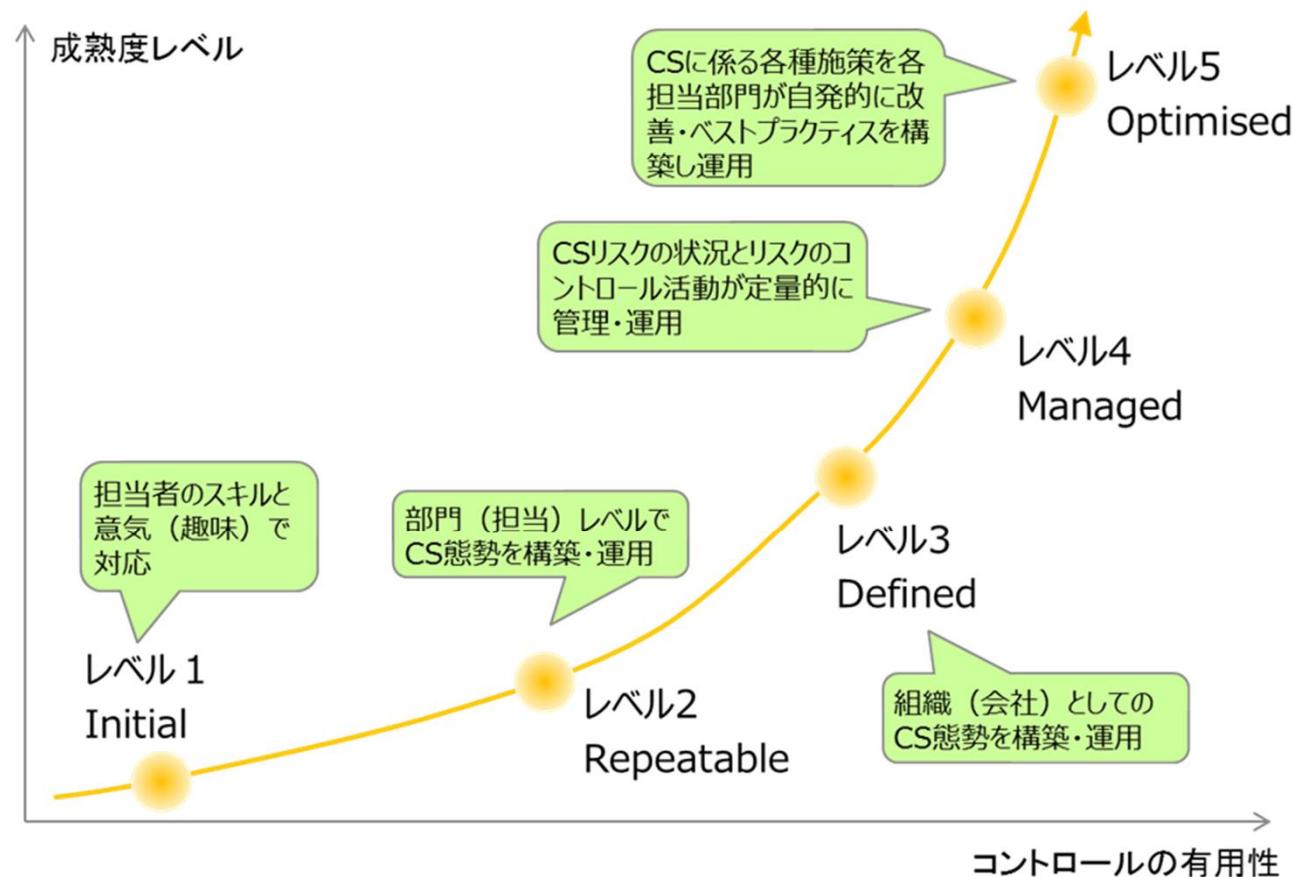
内閣官房及び**重要インフラ所管省庁**は、重要インフラ事業者等の経営層に対して情報セキュリティに関する意識を高めるように**働きかけを行う**とともに、そのような**働きかけを通して知見を得て**、重要インフラ防護施策を実態に即した実効的なものとする。



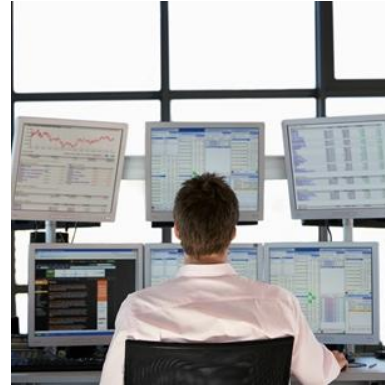
2. 金融機関のサイバーセキュリティへの取組み

金融機関のサイバーセキュリティ管理態勢の成熟度は？

- ▶ 金融機関全体としてサイバーセキュリティ管理態勢整備が進む一方で、金融機関間の格差は大きく(レベル1? ~ 5?)、その差は広がる傾向にある。



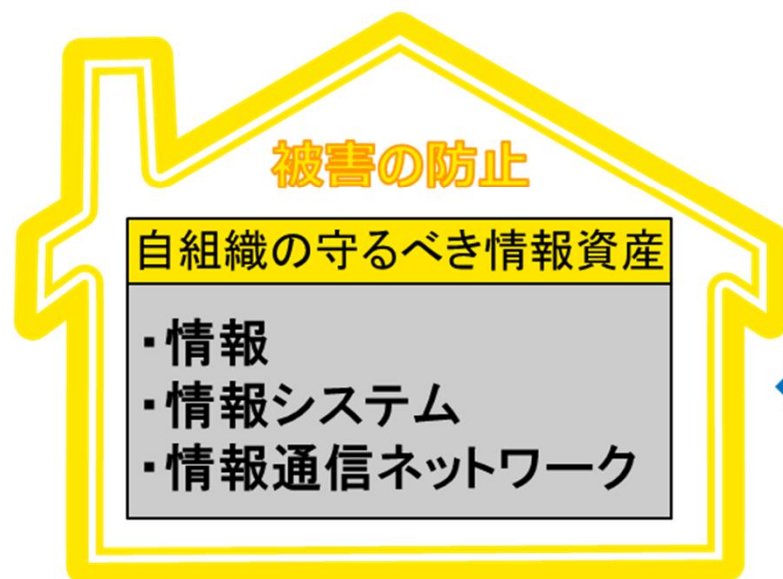
今、金融機関の現場では



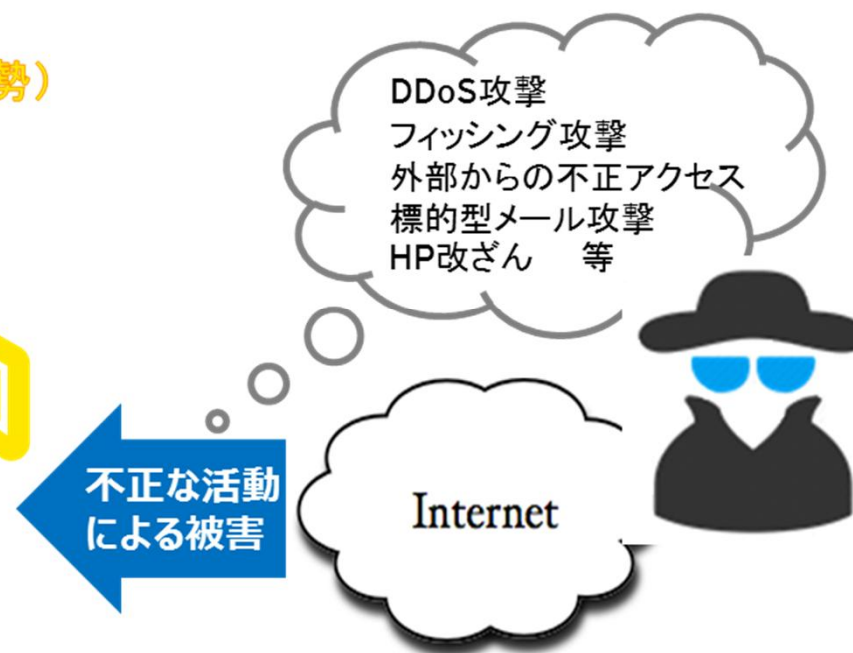


3. サイバーセキュリティ管理態勢の整備に向けて

サイバーセキュリティ (自組織のサイバーセキュリティ管理態勢)

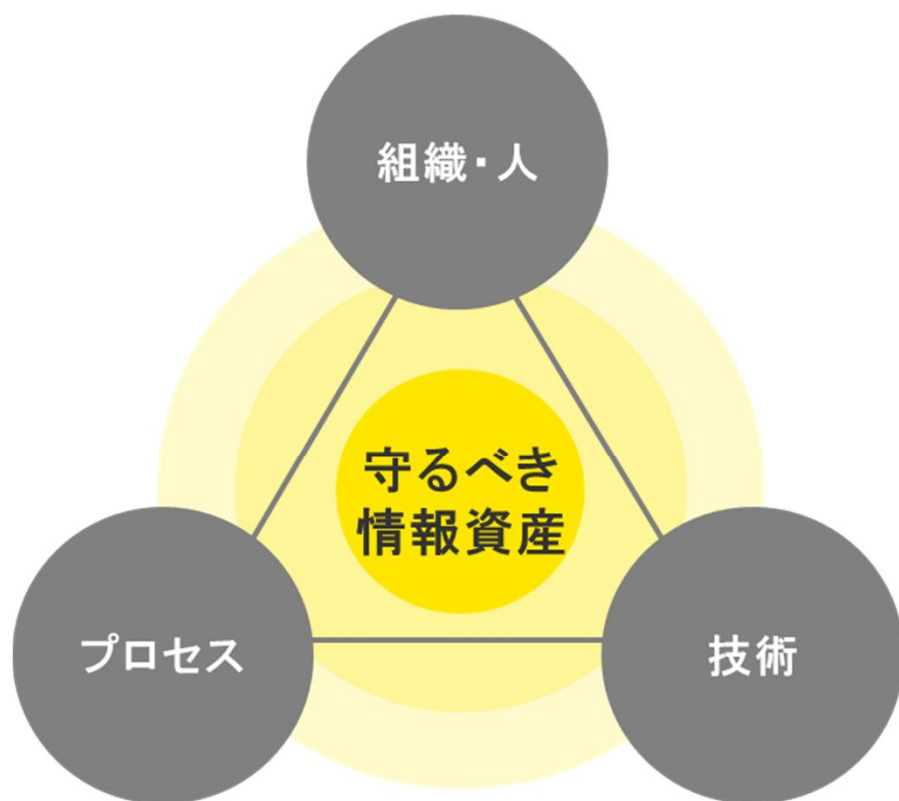


想定されるサイバー攻撃



サイバーセキュリティ管理態勢

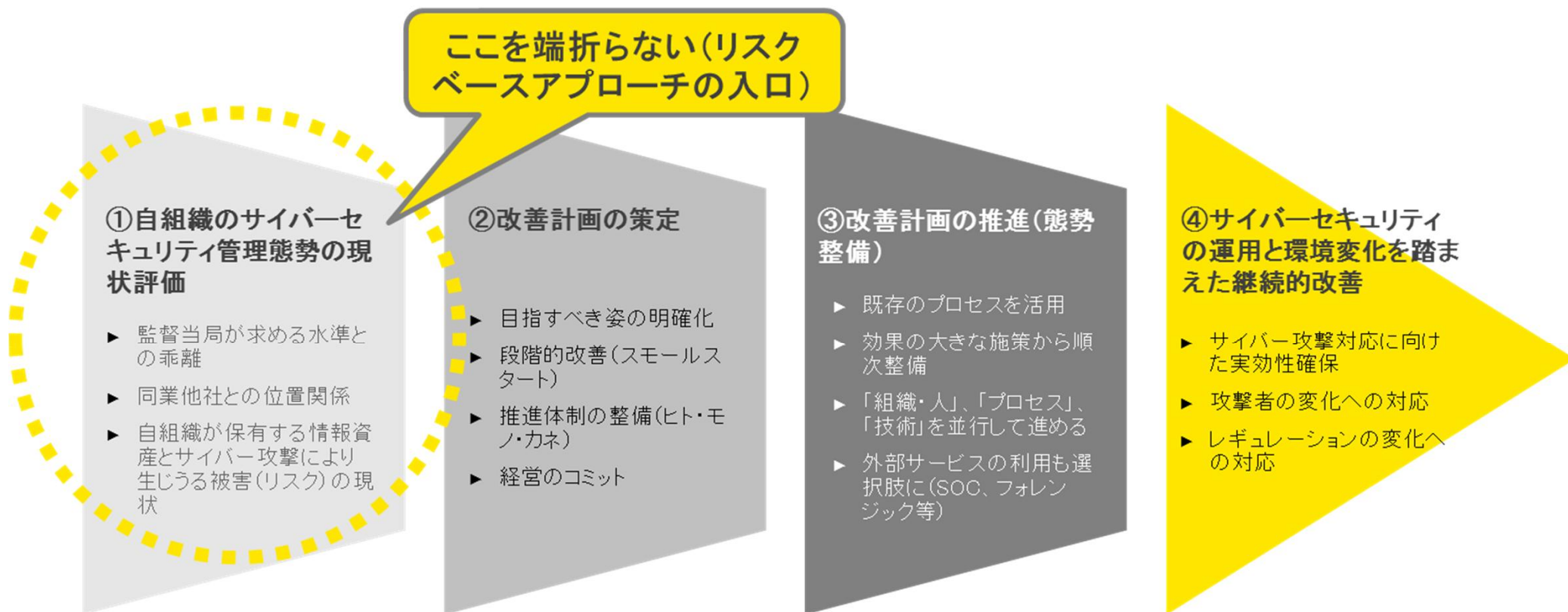
- ▶ サイバー攻撃による脅威に適切に対応するためには、「組織・人」、「プロセス」、「テクノロジー」の3つのパラメータがバランス良く構成されたサイバーセキュリティ管理態勢の構築が肝要です。



組織・人	<ul style="list-style-type: none">▶ 経営のコミットとガバナンス(適切な資源(人・モノ・金)投入・マネジメント状況のモニタリングなど)▶ サイバーセキュリティ対応に係る役割・責任の整備と文書化(専門の対策チームの設置、外部委託先管理など)▶ セキュリティ意識の向上(教育・研修・訓練など) 等
プロセス	<ul style="list-style-type: none">▶ 半期/年単位のセキュリティ向上活動プロセスの整備▶ 平時の活動プロセス(情報収集・分析・評価など)の整備▶ 有事の活動プロセス(インシデントレスポンス態勢)の整備等
技術	<ul style="list-style-type: none">▶ 自社のサイバーセキュリティリスクを考慮した、適切な防御策(セキュリティセンサー等)の導入▶ システムの入口、内部、出口での多層防御の実施▶ サイバー攻撃を想定したITインフラの適切な運用 等

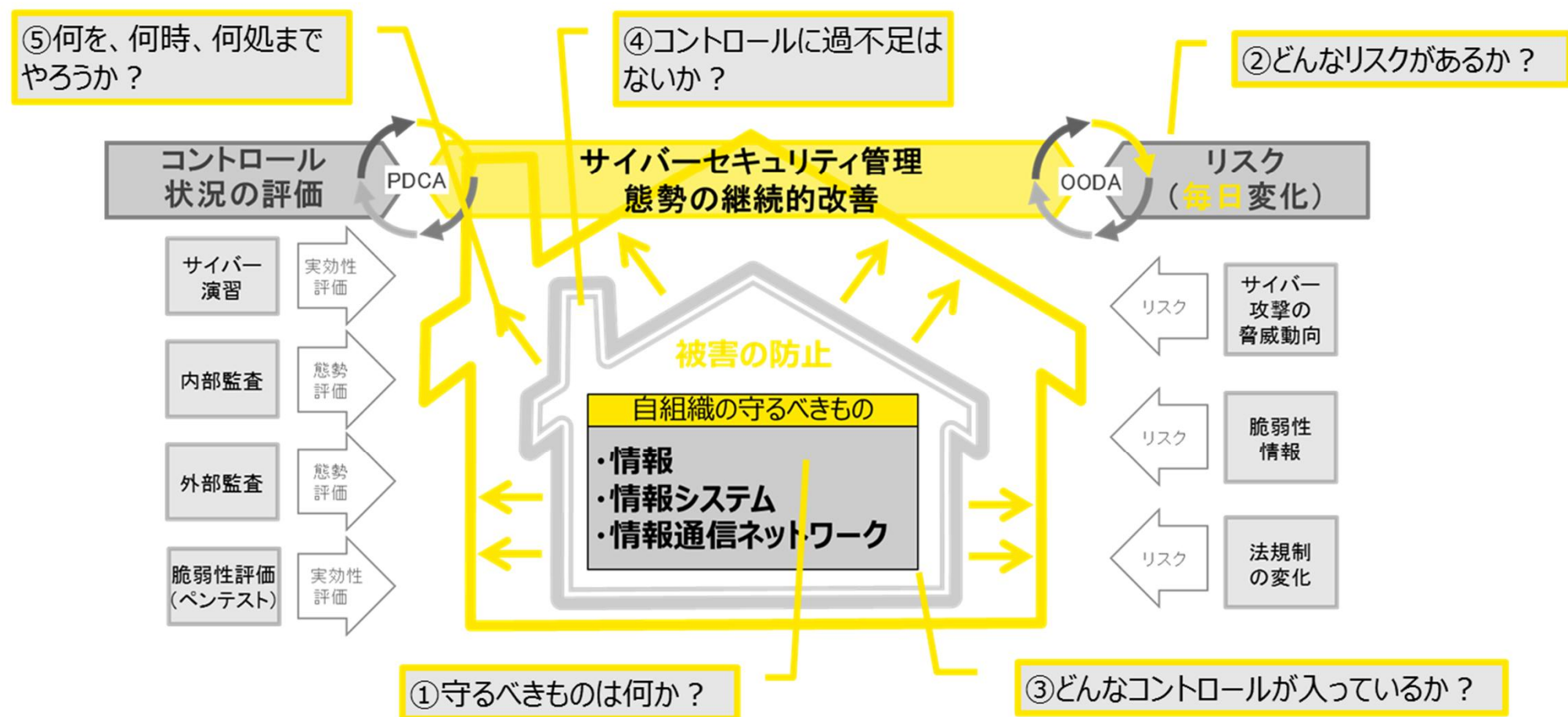
サイバーセキュリティ管理態勢整備へのステップ

- ▶ サイバーセキュリティ管理態勢の整備は、次の4ステップで進めます。
- ▶ 自組織の現在地(Start)と目指すべき姿(Goal)、投入するリソース(社内・社外)により、改善に要する時間・コストが変わります。



サイバーセキュリティ管理態勢整備へのステップ

- ▶ リスクアセスメントのアプローチ(①～⑤)を端折らずに実施。



(まとめ)サイバーセキュリティ管理態勢構築に向けたポイント

- ▶ **サイバー攻撃の対象を明確化 → リスク評価 → リスク低減策を検討**
 - ▶ 守るもの(業務の継続、重要情報、お金など)は何か、どのような攻撃者から、どのように(手段)守るか
- ▶ **サイバーセキュリティ全体を俯瞰し、自組織の現在地を把握**
 - ▶ サイバーセキュリティを構成する「ガバナンス」・「マネジメント」・「オペレーション」全体を対象に
 - ▶ サイバーセキュリティのイネーブラである「組織・人」・「プロセス」・「技術」を切り口に
 - ▶ 具体的活動状況をたな卸し・把握(モレは無いのか、深度は十分か)
- ▶ **経営層による意思決定と戦略の遂行**
 - ▶ サイバーセキュリティ戦略は経営計画(中計など)に組み込み、経営主導で推進
 - ▶ 「ガバナンス」・「マネジメント」・「オペレーション」を適切なサイクル・バランスで運用

EYについて

EYは、アシュアランス、税務、トランザクション及びアドバイザリーなどの分野における世界的なリーダーです。私たちの深い洞察と高品質なサービスは、世界中の資本市場や経済活動に信頼をもたらします。私たちはさまざまなステークホルダーの期待に応えるチームを率いるリーダーを生み出していきます。そうすることで、構成員、クライアント、そして地域社会のために、より良い社会の構築に貢献します。

EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバル・ネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。詳しくは、ey.comをご覧ください。

新日本有限責任監査法人について

新日本有限責任監査法人は、EYの日本におけるメンバーファームであり、監査および保証業務を中心に、アドバイザリーサービスなどを提供しています。詳しくは、www.shinnihon.or.jpをご覧ください。

© 2017 Ernst & Young ShinNihon LLC.
All Rights Reserved.

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務及びその他の専門的なアドバイスを伴うものではありません。新日本有限責任監査法人及び他のEYメンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家にご相談ください。

Contact

新日本有限責任監査法人
金融アドバイザリー部
サイバーセキュリティチーム
Tel: 03 3503 1138

Japan FSO Cybersecurity Leader
シニアマネージャー
小出 哲也
E-mail: koide-ttsy@shinnihon.or.jp

