サイバーセキュリティへの取組み

公益財団法人 金融情報システムセンター

FISCの概要

公益財団法人 金融情報システムセンター
（FISC：The Center for Financial Industry Information Systems）

金融情報システムに関連する各種の課題（技術、利活用、管理態勢、脅威と防衛策等）について総合的な調査研究を行うことを目的として、銀行、証券会社、保険会社、コンピュータメーカー、情報処理会社等の出捐により大蔵大臣（当時）の許可を得て、1984年11月に財団法人として設立。2011年4月に内閣総理大臣の認定を受け公益財団法人に移行しました。

会員構成

正会員　　531機関　(うち金融機関515)

（都市銀行、信託銀行、地方銀行、第二地方銀行、信用金庫、信用組合、労働金庫、農林中央金庫、各都道府県信連、商工組合中央金庫、外国銀行、その他銀行、生命保険会社、損害保険会社、証券会社、銀行系カード会社、電気通信・情報通信会社メーカー、情報システム会社等）

賛助会員　113機関　(うち金融機関27)

合計　　644機関（2017年3月末現在）

1　サイバー攻撃の動向

- ✓ サイバー攻撃の手口は、日々、高度化かつ巧妙化しつづけている
- ✓ 変化するサイバー攻撃に対し、迅速かつ確実に対応するための態勢整備が必要

1　サイバー攻撃の動向

■　金融機関等におけるサイバー攻撃の脅威と攻撃例

対象	脅威	攻撃の例	内容
金融機関等	金融機関・金融市場インフラの機能停止	DoS攻撃 DDoS攻撃	ネットワーク上に配置されたサーバーやPC、ネットワークを構成する機器や回線等のネットワークリソースに対して、サービスを提供できないようにする攻撃。
		Webサイトの改ざん	Webサイトで使用しているソフトウェアや独自に開発されたアプリケーションに存在する脆弱性の悪用や、管理者権限の乗っ取り等により、Webサイトを意図しない状態に変更する攻撃。
		マルウェア（標的型攻撃等）	電子メールやWebサイトの閲覧等で悪意のある不正プログラムをPCやサーバー等の機器に感染させることにより、システムやデータの破壊・改ざん等を行う攻撃。
	機密漏えい	マルウェア（標的型攻撃等）	電子メールやWebサイトの閲覧等で悪意のある不正プログラムをPCやサーバー等の機器に感染させることにより、情報の窃取を行う攻撃。
		脆弱性の悪用	ターゲットのシステムや使用しているソフトウェアに存在する脆弱性を悪用し、情報の窃取を行う攻撃。
	不正送金等の不正取引	マルウェア（標的型攻撃等）	電子メールやWebサイトの閲覧等で悪意のある不正プログラムをPCやサーバー等の機器に感染させることにより、送金等の取引に係る操作手順等を盗み取り、不正な送金指図等の処理を行う攻撃。
顧客		フィッシング	金融機関等からのメールを装い、メールの受信者に偽のホームページにアクセスするよう仕向け、そのページにおいてIDやパスワード等の重要情報を入力させるなどして、不正に入手した情報により不正取引を行う攻撃。
		マルウェア	・メール等により、インターネットバンキングの利用者をマルウェアに感染させ、正規サイトへのログイン時に偽画面（ポップアップ画面等）を表示し、IDやパスワード等の重要情報を入力させるなどして、不正に入手した情報により不正取引を行う攻撃。
			・メール等により、インターネットバンキングの利用者をマルウェアに感染させ、利用者によるインターネットバンキングへのログインを契機に、利用者に気づかれないよう取引を乗っ取り不正取引を行う攻撃。

出所：金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）

1　サイバー攻撃の動向

攻撃者・標的・目的は、「多様化」している

国家・宗教
破壊・脅し

犯罪グループ
情報・金銭

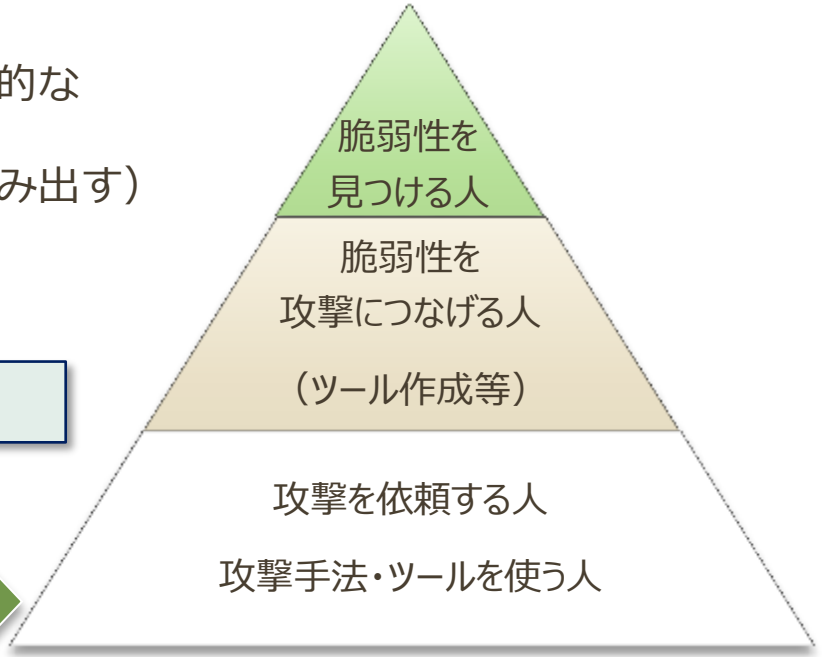
市民レベル
いやがらせ

サイバー攻撃は、「ビジネス化」「国際化」している

・攻撃者の多様化を生み出す闇サイト
（高校生によるサイバー攻撃に使われた）
・情報・マルウェア・ボットネットを売買する国際的なブラックマーケット
（マルウェアの流通や、新たなサイバー犯罪を生み出す）
・プロキシサーバー業者の不正
（不正送金に不正に利用され、複数業者が摘発）

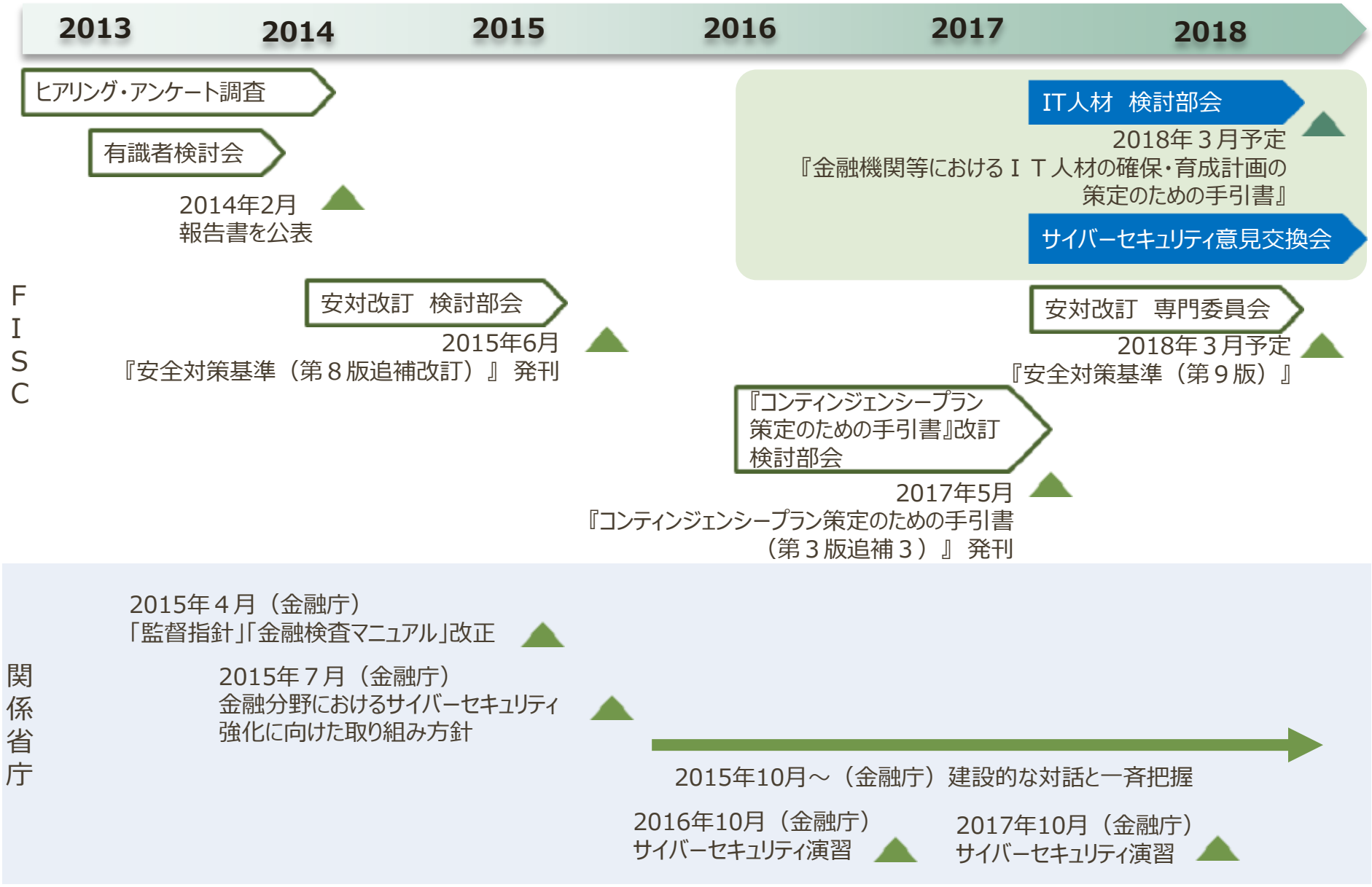
サイバー攻撃は、「分業化」している

・攻撃者は、必ずしも高度な技術者集団のみで構成されているとは限らない



この層が圧倒的に多い

2　FISCの取組み



2　FISCの取組み

金融庁動向：『金融分野におけるサイバーセキュリティ強化に向けた取組方針』

基本的考え方

- ✓ 金融分野のサイバーセキュリティ対策の強化には、**官民が一体となって取り組んでいく**ことが重要。
- ✓ このため金融庁は、金融機関との間で、サイバーセキュリティ確保という共通目的を有しているとの理解の下、**建設的な対話を日常的に重ねていくことを目指す**とともに、行政当局の立場から**金融分野のサイバーセキュリティ強化に貢献する**ため、以下の５項目に取り組んでいく。

５つの方針

1．サイバーセキュリティに係る金融機関との建設的な対話と一斉把握
2．金融機関同士の情報共有の枠組みの実効性向上
3．業界横断的演習の継続的な実施
4．金融分野のサイバーセキュリティ強化に向けた人材育成
5．金融庁としての態勢構築

2　FISCの取組み

金融庁動向：『金融分野におけるサイバーセキュリティ強化に向けた取組方針』

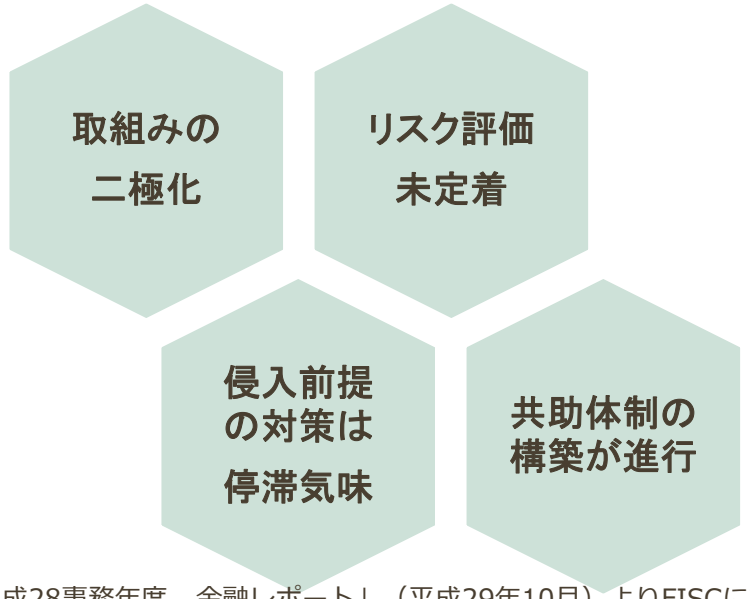
■サイバーセキュリティに係る金融機関との建設的な対話と一斉把握

✓ ヒアリング項目

- サイバーセキュリティに関する経営陣の取組み
- リスク管理の枠組み
- サイバーセキュリティリスクへの対応態勢
- コンティンジェンシープランの整備と実効性の確保
- サイバーセキュリティに関する監査

■　**態勢整備が進んでいる金融機関に共通した取組み**

■　**建設的な対話と一斉把握からわかった課題**



出所：金融庁「平成28事務年度　金融レポート」（平成29年10月）よりFISCにて作成

2　FISCの取組み

平成２９年度の取組み

■「サイバーセキュリティ意見交換会」の開催

各金融機関の実務者を対象に講義による知識共有とグループディスカッションで活発な意見交換を実施。
継続して更なる深耕・展開の必要性がある。

■サイバーセキュリティ人材の確保・育成に関する考慮事項の作成

『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』（平成30年3月発刊予定。以下、ＩＴ人材手引書）において、サイバーセキュリティ人材に関する考慮事項を執筆。

平成３０年度の予定

■「サイバーセキュリティワークショップ」の開催
（旧：サイバーセキュリティ意見交換会）

・年間11回開催：東京（２回）、札幌、仙台、長野、金沢、名古屋、大阪、広島、松山、福岡
・各協会団体と連携強化し態勢整備強化の底上げを図る

■サイバーセキュリティ人材の確保・育成に関する事例の提供

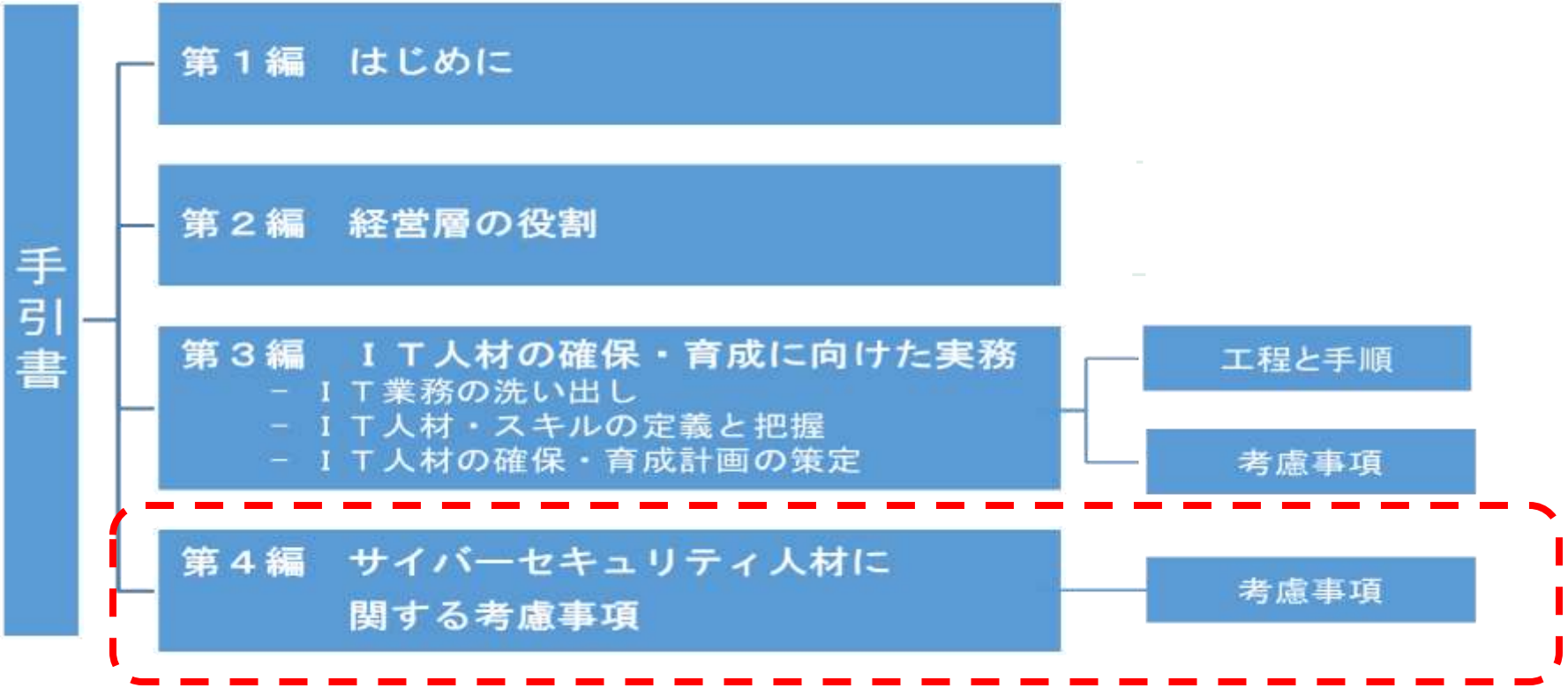
全国説明会を実施するとともに、『ＩＴ人材手引書』の参考となるようなサイバーセキュリティ人材の　確保・育成に関して金融機関での取組みを調査し、その具体事例をレポート等にて還元する。

2　FISCの取組み

■『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』

✓ 経営戦略・事業戦略とシステム戦略は不可分一体となっており、ＩＴを担う人材の役割はこれまで以上に大きくなっている。

① 業務のIT化・多様化
② 新しい技術やサービスへの対応
③ **サイバーセキュリティへの対応**
④ 外部委託先を管理できる人材の育成



2　FISCの取組み

■『金融機関等におけるＩＴ人材の確保・育成計画の策定のための手引書』

✓ サイバーセキュリティ人材については、IT業務と異なるスキルが求められることと人材の数と質の不足が喫緊の課題となっていることから、第4編としてサイバーセキュリティ人材を確保・育成するうえでの考慮事項を記載。

考慮事項（例）

- ✓ サイバー攻撃対応に必要な業務・役割の洗い出しと業務の細分化
- ✓ サイバーセキュリティ人材の定義と把握
  - ①　組織の責任者等の必要性
  - ②「橋渡し人材層」の役割と必要性　等
- ✓ サイバーセキュリティ人材に求められるスキル
  - ①　IT知識
  - ②　サイバーセキュリティ固有の知識
  - ③　金融業務知識と自機関の情報システムに関する知識
- ✓ サイバーセキュリティ人材の確保・育成について
  - ①　産学連携に基づく教育
  - ②　訓練・演習等におけるスキル向上　　等

【参考】情報セキュリティ10大脅威 2018

■「情報セキュリティ 10 大脅威 2018」　　NEW：初めてランクインした脅威

昨年順位	「個人」の 10 大脅威	順位	「組織」の 10 大脅威	昨年順位
1 位	インターネットバンキングや クレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺 NEW	ランク外
3 位	スマートフォンやスマートフォン アプリを狙った攻撃の可能性	4 位	脆弱性対策情報の公開に伴い 公知となる脆弱性の悪用増加	ランク外
4 位	ウェブサービスへの不正ログイン	5 位	セキュリティ人材の不足 NEW	ランク外
6 位	ウェブサービスからの個人情報の窃取	6 位	ウェブサービスからの個人情報の窃取	3 位
8 位	情報モラル欠如に伴う犯罪の低年齢化	7 位	IoT 機器の脆弱性の顕在化	8 位
5 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切な管理	9 位	サービス妨害攻撃による サービスの停止	4 位
ランク外	偽警告 NEW	10 位	犯罪のビジネス化 （アンダーグラウンドサービス）	9 位

出所：独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威 2018」

4　まとめ

サイバー攻撃の動向

- ✓ サイバー攻撃の手口は、高度化・巧妙化
- ✓ 被害件数は増加、被害規模は拡大傾向
- ✓ 攻撃者のすそ野は広がり、サイバー攻撃前提での対策が必要

サイバーセキュリティの取組み

※自組織の態勢・対策等の状況を認識し、基本的な対策を適切に実施することで、サイバー攻撃への対応力を向上させる

サイバーセキュリティ向上の一助として、
FISCの各種ガイドラインをご活用ください

ご清聴ありがとうございました

公益財団法人　金融情報システムセンター
https://www.fisc.or.jp/