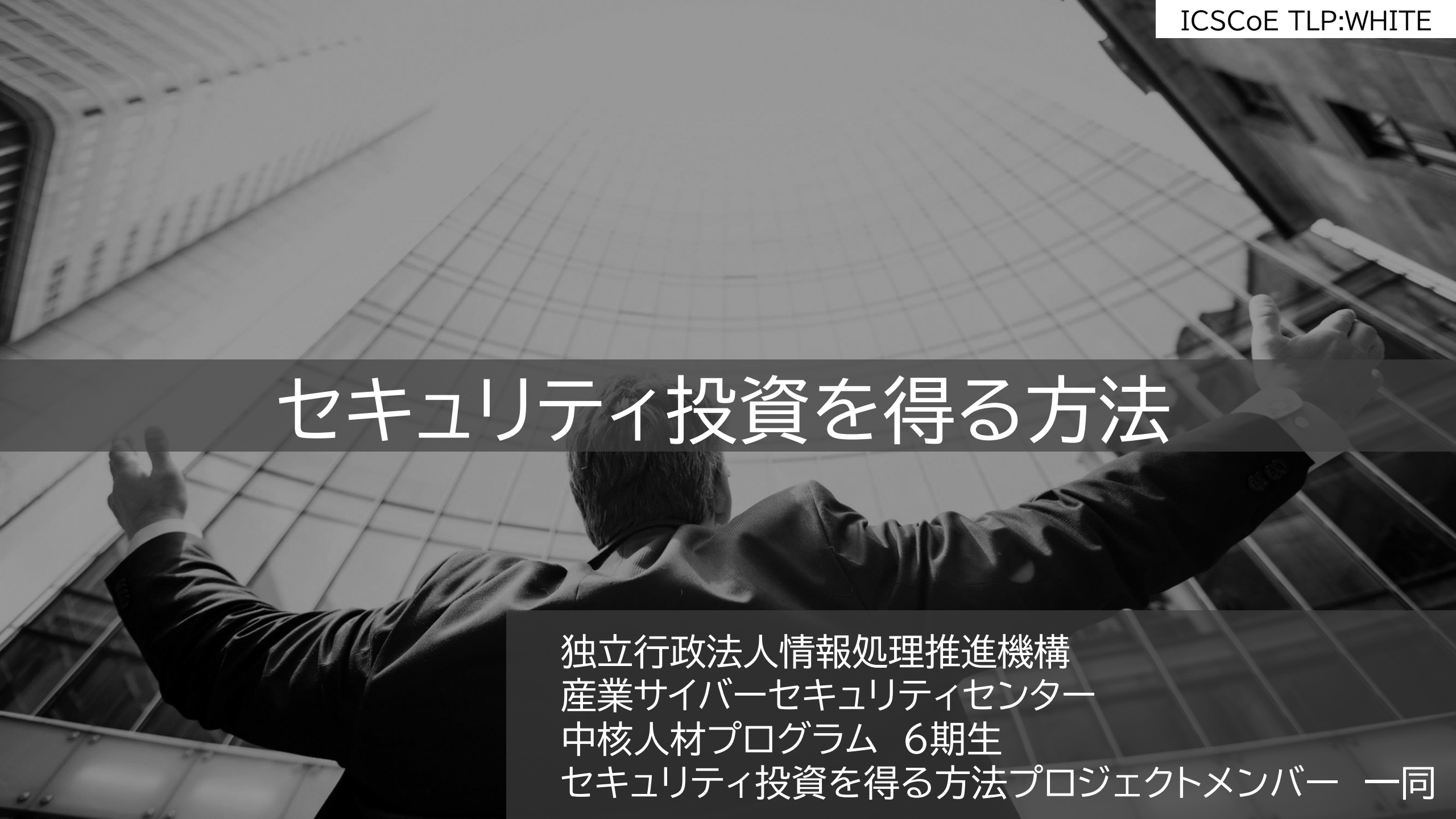


セキュリティ投資を得る方法

独立行政法人情報処理推進機構
産業サイバーセキュリティセンター
中核人材プログラム　6期生
セキュリティ投資を得る方法プロジェクトメンバー　一同

セキュリティはコストか？投資か？

世の中の企業はセキュリティ投資が
できているのか？

セキュリティ投資を得る方法を確立したい

目次

本書について

本書はセキュリティ担当者がセキュリティ投資を継続的に得るために
活用できる方法、ツール、ベストプラクティスをまとめた参考資料です。

本書では
セキュリティ＝サイバーセキュリティとします。

投資は一般的には金銭的な意味で使用されることが多いですが、
本書でのセキュリティ投資は**人の稼働(工数)**も含むものとします。

本書では
社内を守るセキュリティに従事する担当者、投資提案を行う方々を
対象とします。

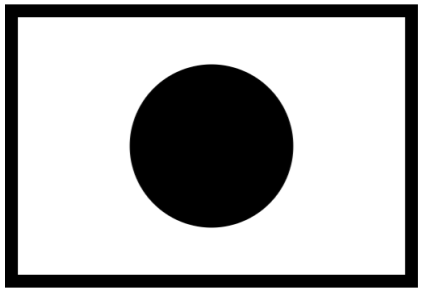
CSIRT : Computer Security Incident Response Team
FSIRT : Factory Security Incident Response Team

PSIRT : Product Security Incident Response Team
DSIRT : Digital Service Security Incident Response Team

本書について ▶ 免責事項

- 本書は企業インタビューを元に作成していますが、インタビュー数は少なく
  インタビュー先企業には偏りがあり、統計的に有意なものではありません。
- 本書の内容は一つのプロジェクトの中で出した一つの結論としての参考情報としてご利用ください。
- 本書は単に情報として提供され、内容は予告なしに変更される場合があります。
- 本書に誤りがないことの保証は一切ないものとします。
- 本書の利用によるトラブルに対し、本書著者ならびに監修者は一切の責任を負わないものとします。
- 本作品の内容は本プロジェクトの見解に基づいております。独立行政法人情報処理推進機構
  （IPA）および作成者の所属企業の見解を反映するものではありません。
- 本書の有効期限は、発行日（2023年7月）から2年間とします。

インタビューした企業は16社



日系企業のみ

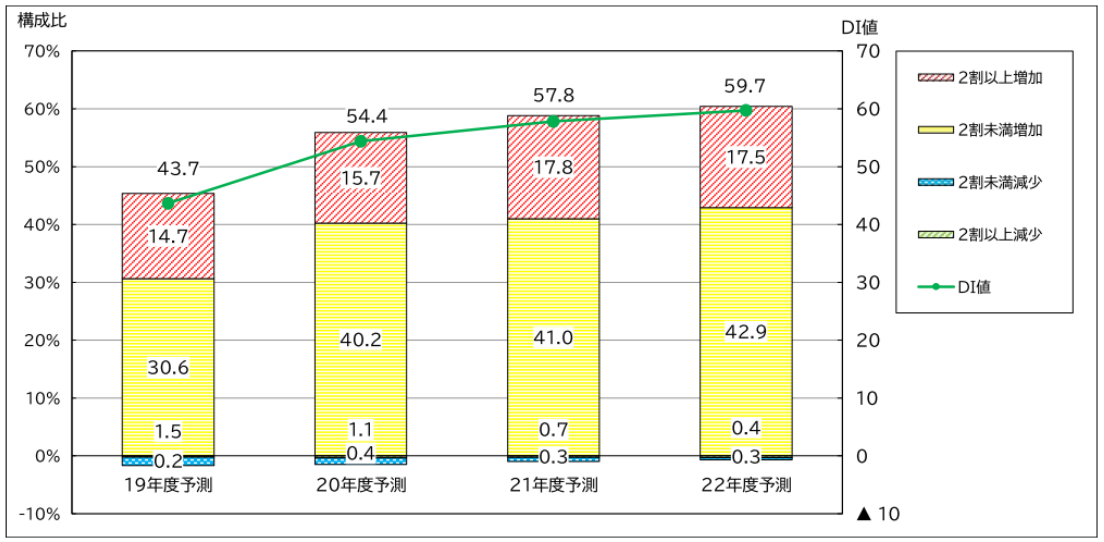
回答者は社内
セキュリティ担当者
および経営層

産業サイバーセキュリティ
センター中核人材育成
プログラム参画企業中心

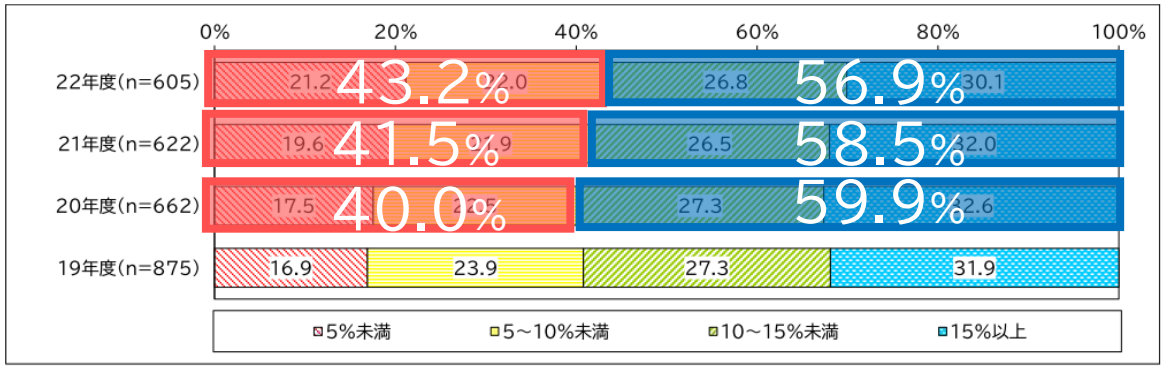
背景と達成目標

背景

図表 4-1-4　今後(3 年後)の情報セキュリティ関連費用の増減予測における DI 値の推移



図表 4-1-1　年度別　IT 予算に占める情報セキュリティ関連費用の割合



ここ3年のIT予算に占める
セキュリティ関連費用の割合は低下

一般社団法人　日本情報システム・ユーザー協会(JUAS)
企業IT動向調査報告書 2023より抜粋

一般社団法人　日本情報システム・
ユーザー協会(JUAS)の調査によると、
セキュリティ関連費用は増加の予測に
なっています。

しかしIT予算に占める情報セキュリティ
関連費用の割合は鈍化の傾向も
見受けられます。

いかなる経営環境にあっても
継続して投資を得るにはどうすれば
よいでしょうか？

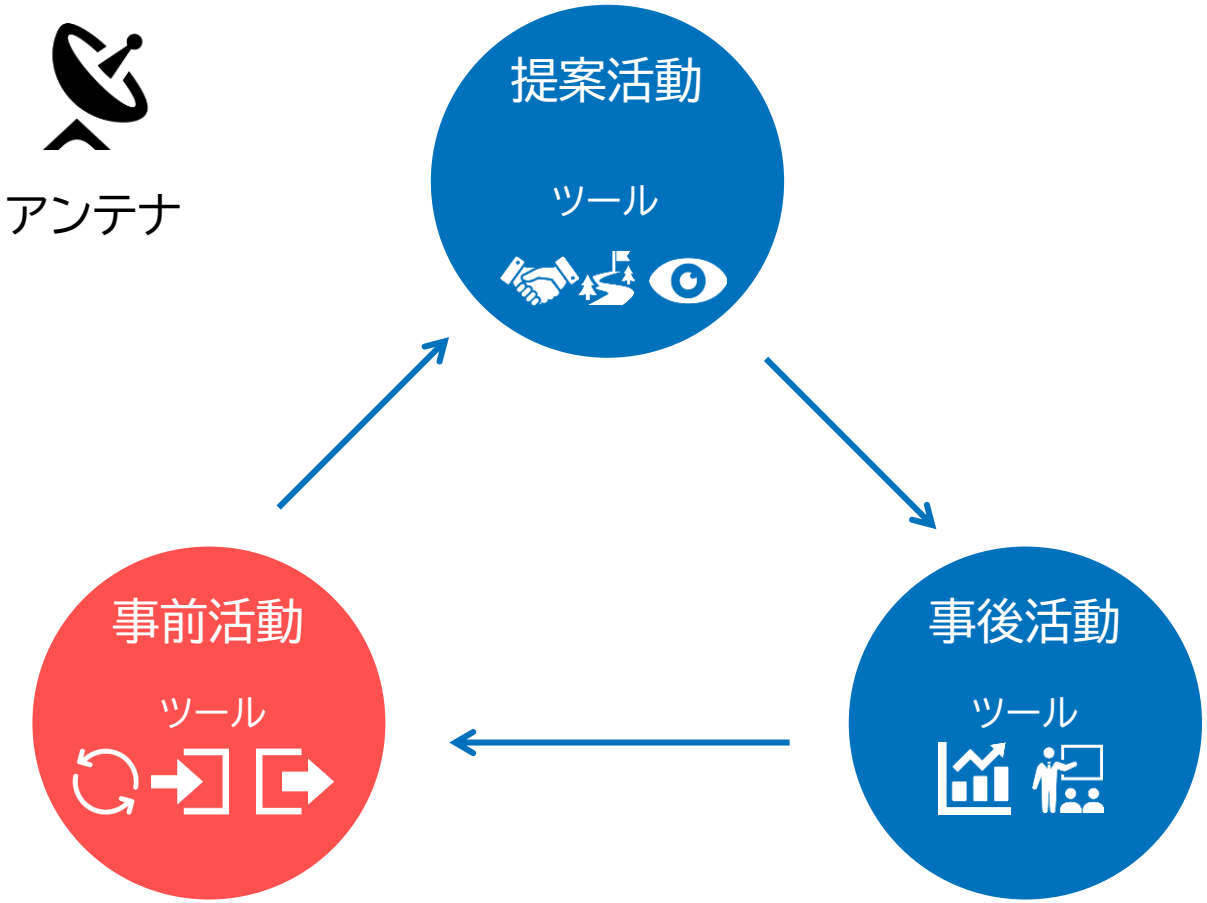
目標

本書では、いかなる経営環境においても経営層や他部署(セキュリティ専門部署でない部署)の方々からセキュリティ投資(予算や協力)を得られる状態を作り出すことを目標とします。

まずはセキュリティ投資をしてもらう相手は経営層とし、
経営層のセキュリティに対する理解を得るための方法を提供します。

セキュリティ投資を得る方法

セキュリティ投資を得る方法



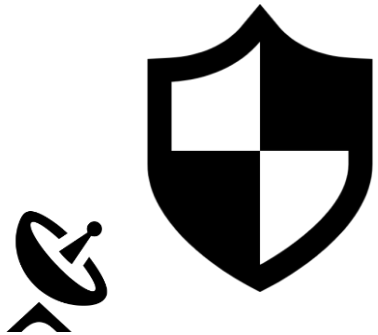
セキュリティ投資を得る方法の全体像を左記に示します。

まず社内外の情報を取得するアンテナがあります。
プロセスを事前活動、提案活動、事後活動に分け、それぞれのツールについて説明していきます。

セキュリティ投資を得る相手は経営層とします。

アンテナ

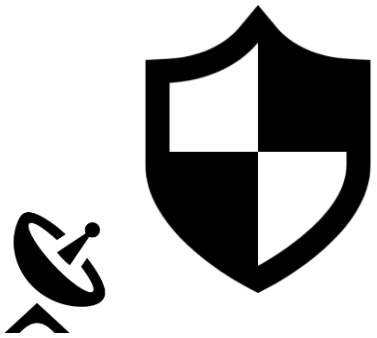
アンテナはこの後の活動全てに共通する情報です。
日頃からセキュリティとビジネスのトレンドにアンテナを
張るようにし、この後で紹介する活動の中で議論する項目に
含めましょう。



セキュリティ

ビジネス

アンテナ



セキュリティ

◆世の中の動向（流行りの攻撃、セキュリティ対策、セキュリティ商品など）
◆同業他社、同規模他社の施策、事例、動向
◆自社内のインシデント状況（未然防止含む）

これらの情報は日系企業においては経営層や関連部署の方々の
セキュリティ意識を高めるために非常に有効な情報です。
特に**他社情報は経営層が参考にしたい情報**です。

セキュリティの情報収集の方法

主な情報収集方法は下記2点です。

WEBサイトやSNS

情報収集コストがほぼ
かからない手法です。
情報源や裏付けなどに
注意しながら収集しま
しょう。

セキュリティの仲間、外部団体、
国際会議、展示会

競合他社であっても
セキュリティ分野では
競合しないことも多いです。
仲間を作りましょう。
ISAC等の団体がある場合は
積極的に活用しましょう。

WEBサイトの例

下記のようなウェブサイトが利用されています。
特に海外の情報は日本より早い(日本の情報が海外の情報を翻訳され
出される場合が多い)ため海外のウェブサイトもチェックするようにしましょう。

分類	サイト名	URL
日々の情報収集	独立行政法人情報処理推進機構	https://www.ipa.go.jp/
	JPCERT コーディネーションセンター	https://www.jpcert.or.jp/
	Security Next	https://www.security-next.com/
	ScanNetSecurity	https://scan.netsecurity.ne.jp/
トリアージの参考	Known Exploited Vulnerabilities Catalog	https://www.cisa.gov/known-exploited-vulnerabilities-catalog
調査資料	一般社団法人 日本情報システムユーザー協会	https://juas.or.jp/
	NPO日本ネットワークセキュリティ協会	https://www.jnsa.org/
	一般社団法人　日本サイバーセキュリティ・イノベーション委員会	https://www.j-cic.com/
海外	BleepingComputer	https://www.bleepingcomputer.com/
	Dark Reading	https://www.darkreading.com/

アンテナ

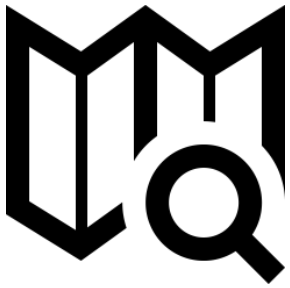
ビジネス

◆ 自社、同業他社のビジネスゴール
◆ 自社、同業他社のビジネス環境
◆ お客様業界の動向（規制、業界標準など）

経営層はセキュリティのことだけを考えているわけではありません。
自社、同業他社のビジネスゴールを達成するために使用される
IT技術を意識することで、経営層の課題に合った提案ができます。

ビジネスの情報収集の方法

主な情報収集方法は下記2点です。



OSINT

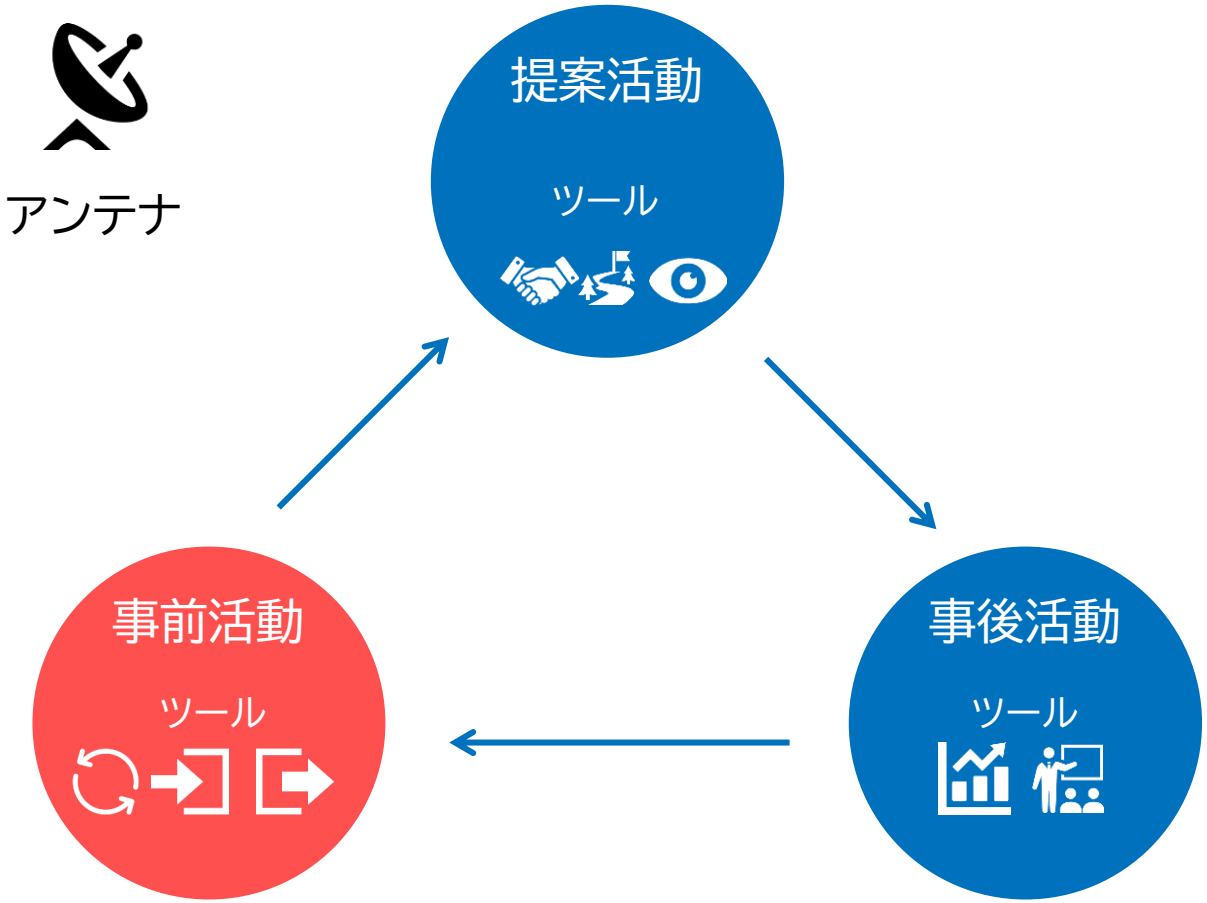
IR情報等の公開情報は
自社、他社ともに有用
な情報源です。
OSINTサービスを利用
するのもよいでしょう。

OSINT:Open Source Intelligence

経営層の言葉

中期計画などの経営層の
言葉は自社の目標と
課題について触れられる
良い機会です。
計画の中にセキュリティの
観点も盛り込めるのが
理想です。

セキュリティ投資を得るプロセス



セキュリティ投資を得るための
方法をプロセスごとに解説します。

以下のプロセスに分解します。
◆事前活動
◆提案活動
◆事後活動

事前活動は全ての活動の起点となるため、
最も重要な活動です。

事前活動

事前活動

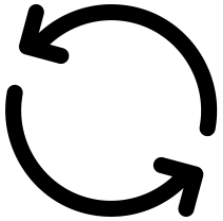
巻き込む

インプット
する

外に
求める

事前活動とは、投資を得たいと
思ったときに投資を得やすくしておく
土壌づくりです。

事前活動では
◆巻き込む
◆インプットする
◆外に求める
の3つのツールを紹介します。

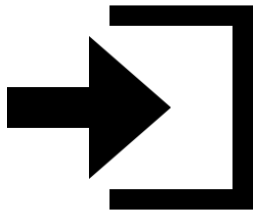


巻き込む、では以下のような手段があります。

◆経営層を入れての会議体を作る
セキュリティ委員会やセキュリティ協議会のような会議体があると当事者意識が向上します。会議体の頻度は月1回以上が望ましく、少なくとも四半期に1回は開催できるようにしましょう。

◆経営層を入れての勉強会
勉強会を行うと理解、関心が深まります。
年1回は開催できるようにしましょう。

◆セキュリティ憲章、標準、ガイドラインなどの社内規定を作る
経営層が関わる規定でセキュリティ対策について考慮することを盛り込んでおけば話がスムーズになります。



インプットする、では以下のような手段があります。

◆年次計画
予め計画されている予算や施策は受け入れられやすいです。
決められるものについては早めに取り掛かりましょう。
不可抗力、不確定要素に対応する予算も入れておきましょう。

◆月次報告
自社の状況（予算執行したもの、セキュリティ目標に対する現在の状況、インシデント事例等）について月次報告をあげるようにしましょう。

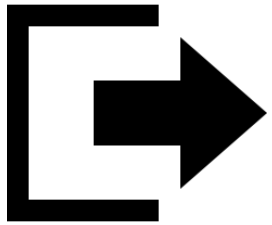
◆3行ニュース（次項に例示）
自社（同業、同規模など）に関わりのあるセキュリティ情報を3行にまとめメールや社内SNSなどで経営層とシェアしましょう。

3行ニュースの例

2023/6/8　DDoS攻撃の予告を受け、Microsoft OneDriveが世界中で停止
https://www.bleepingcomputer.com/news/microsoft/microsoft-onedrive-down-worldwide-following-claims-of-ddos-attacks/
・Microsoft OneDriveが世界中で停止した。
・Microsoftは原因について調査中であると述べている一方で、ロシアに関連があると思われる攻撃集団アノニマススーダンが分散型サービス拒否（DDoS）攻撃で、多くのマイクロソフトのサービスをダウンさせたと述べた。
・Microsoftによると影響を受けるURLは”onedrive.live.com”のみでデスクトップクライアント、同期クライアント、Officeクライアントを使用したOneDriveサービスへのアクセスは影響を受けないと述べている。

※ポイント：情報源を明らかにし、自身の主観を入れないようにしましょう。

3行ニュースは経営層へのインプットとして使えるだけでなく
以下の点で発信者自身の教育としても使えます。
◆世の中のセキュリティ動向がわかる
◆調べる習慣がつく
◆報告の手法を学べる



外に求める、では以下のような手段があります。

◆外部団体
経営層がセキュリティに関する外部団体に所属するチャンスがあれば積極的お願いしましょう。セキュリティに対する関心が大きく高まります。

◆他社との情報交換
セキュリティ施策については自社内に基準や答えが無いこともあり、個人的なつながりも含め積極的な情報交換ができるようにしましょう。

◆外部への発信
セキュリティ報告書やセキュリティ方針、対策などを外部に
発信しましょう。社会に約束したことでセキュリティを自分事にできます。

提案活動

提案活動

提案活動とは、投資を得る際に行う
投資提案です。経営会議や稟議説明など
が提案活動にあたります。

提案活動では
◆抱き合わせ
◆シナリオ
◆第三者の視点
の3つのツールを紹介します。

社内で流行りや勢いのあるIT施策と合わせて
投資提案を行うとよいでしょう。

例えば以下が挙げられます。
◆DX
◆働き方改革
◆インフラ更新時
また、データ収集による故障予知、業務効率化の利用も考えられます。

セキュリティの考えられていないDXや働き方改革は、
DXや働き方改革ではないと断言してもよいでしょう。

提案の必要性、妥当性、客観性を筋道立てて示すことが重要です。

◆ 中長期計画の中で、今回の提案がどういった位置づけか
◆ どういった攻撃が流行っていて、どのように防ぐか
◆ なぜその防御手法が最適か
　などを盛り込むようにしましょう。

自社だけでなく3C（顧客、自社、競合）の観点も入れるようにしましょう。

提案活動 ▶ 第三者の視点

セキュリティベンダからの情報やレーティングサービスは
世の中、他社との比較に役立ちます。

外部の専門家による分析・指摘により、社内検討とは異なる観点を
得られることもあります。

世の中の動向、他社情報は日本の経営層が参考にする情報です。
レーティングサービスを利用している場合は参考情報として提案活動
で利用してもよいでしょう。

事後活動

効果の
見える化

社会への
還元

事後活動はセキュリティ施策を行った結果をフィードバックします。

事後活動では
◆効果の見える化
◆社会への還元
の2つのツールを紹介します。

事後活動は次の投資および次の事前活動につながります。

事後活動 ▶ 効果の見える化

効果の見える化の例です。
◆SOARの導入によるインシデント対応の削減工数、
◆メールサーバへの対策で防御した標的型メールの数
◆EDR導入によるインシデントの短縮時間
定量的に表現できることが望ましいですが定量的にできない部分は
定性的でも表現するようにしましょう。

特にインシデントとして発生していないが、
どれだけ攻撃を受けていてどれだけ防げているか、
実際に被害を被っていたらどれだけの損害になっていたか
を示すことは有効です。

事後活動 ▶ 社会への還元

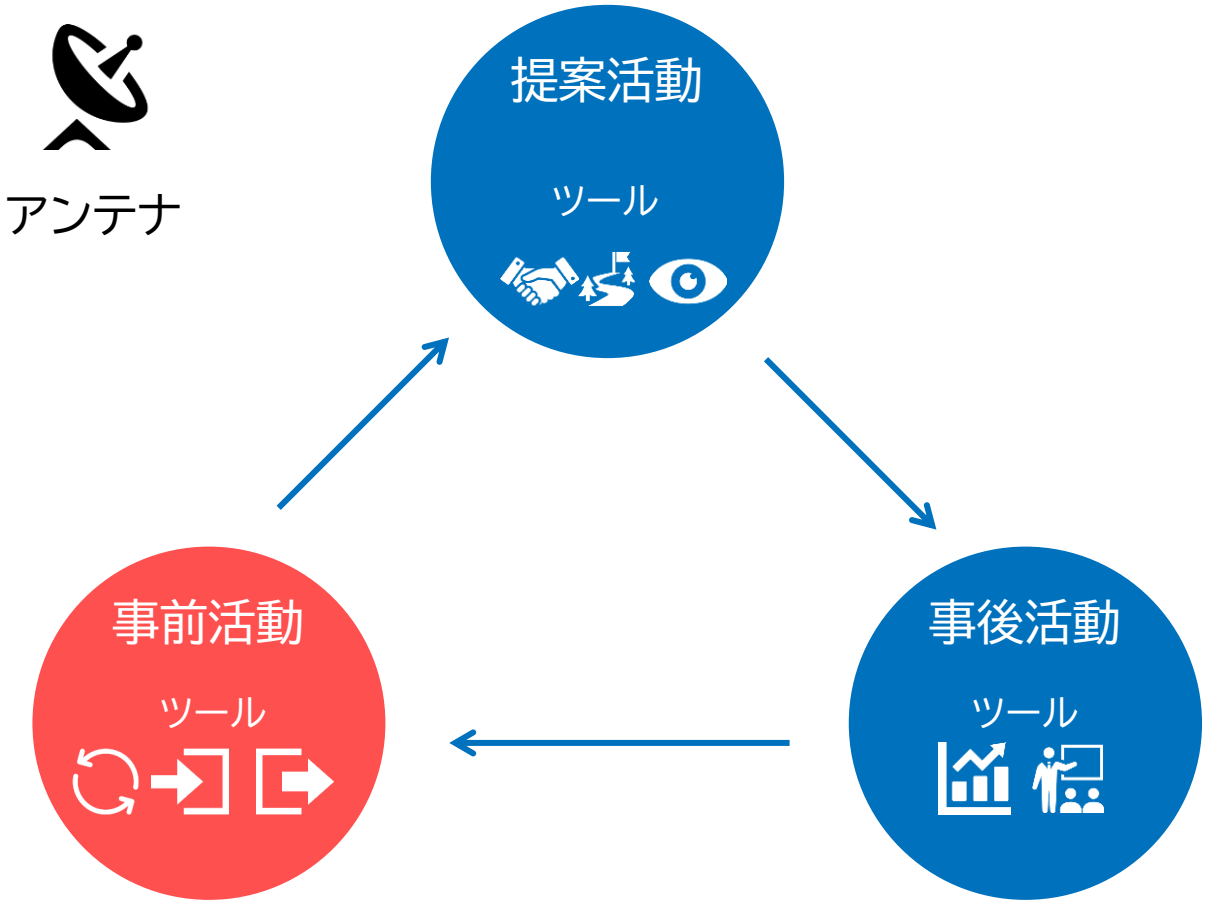
外部団体、国際会議等で成功事例や克服した悩みなどを
共有しましょう。

情報は発信するところに集まってきます。
機微な情報に注意しつつ積極的に外部に発信しましょう。

情報発信することでセキュリティの仲間を増やすことにも役立ちます。

まとめ

セキュリティ投資を得る方法



◆セキュリティ投資を得る方法を
- アンテナ
- 事前活動
- 提案活動
- 事後活動

に分けて説明しました。

◆セキュリティ投資の土壌となる事前活動が最も重要です。

◆経営層のセキュリティに対する理解、関心を高めましょう。

まとめ

プロセス	ツール	具体例
アンテナ 	◆ セキュリティ	WEBサイト
		SNS
		セキュリティの仲間、外部団体、国際会議、展示会
	◆ ビジネス	OSINT、IR情報等の公開情報
		中期計画などの経営層の言葉
事前活動 	◆ 巻き込む	経営層を入れての会議体
		経営層を入れての勉強会
		セキュリティ憲章、標準、ガイドラインなどの社内規定
	◆ インプットする	年次計画（不可抗力、不確定要素に対応する予算計上）
		月次報告（自社のセキュリティ状況）
		3行ニュース（自社関連セキュリティ情報）
	◆ 外に求める	外部団体（セキュリティに関する外部団体）
		他社との情報交換
		外部への発信（環境報告書と同じようにセキュリティ報告書等）
提案活動 	◆ 抱き合わせ	DXと合わせる
		働き方改革と合わせる
		インフラ更新時と合わせる
	◆ シナリオ	中長期計画の中で、今回の提案がどういった位置づけか
		どういった攻撃が流行っていて、どのように防ぐか
		なぜその防御手法が最適か
	◆ 第三者の視点	セキュリティベンダ
		レーティングサービス
		外部専門家の活用
事後活動 	◆ 効果の見える化	SOARの導入によるインシデント対応の削減工数
		メールサーバへの対策で防御した標的型メールの数
		EDR導入によるインシデントの短縮時間
	◆ 社会への還元	外部団体、国際会議等で成功事例や克服した悩みなどを発信 （情報は発信するところに集まってくる。）

終わりに

終わりに

突然ですが、あなたの上司から
「10分後の経営会議にて10分間の時間が取れた。
セキュリティに対する当社の進むべき方向性について説明してくれ」
と言われた場合、あなたは対応できますか？

経営層や他部署を巻き込むチャンスはどこにあるかわかりません。
確実に掴めるように日々準備をしておき、会社全体のセキュリティ向上
に取り組みましょう。

終わりに

セキュリティ投資を得る方法、というテーマで説明
しましたが、結局のところ投資を決断するのは
人です。

最終的には情熱が必ず伝わります。

会社を守りたい、という気持ちを大事にし、
経営層、他部署の方々にセキュリティが自分事に
なってもらえるようコミュニケーションを図りましょう。

あとがきに代えて

本書では予算や費用ではなく「投資」という言葉にこだわって使用しました。

投資の英語 investment の語源は
in（中に） + vest（服のベスト）であると言われています。

一説によると、商人がきれいな衣服を身にまとうことによって
将来的な利益を得るためにお金を出す、という意味から来ているとのことです。

これは「きれいな身なり＝信用」に対してお金や時間をかける行為です。

セキュリティもビジネスをするうえで社会、お客様からの「信用」を得るために必要なもの、
つまり**セキュリティは投資である**と、筆者は考えています。

謝辞

本書の作成にあたり、独立行政法人情報処理推進機構
産業サイバーセキュリティセンター　中核人材育成プログラム講師の、
越島一郎先生、佐々木弘志先生には本書の元となるプロジェクトのメンター・
講師として、ご指導・ご助言、ご支援を賜りました。改めて御礼申し上げます。
諸般の事情により、お名前を挙げることはできませんが、
インタビューでお世話になりました皆様にこの場を借りて心より
御礼申し上げます。
そして、本書の作成や本プロジェクトをともに実施した、メンバーの皆様にも深
く御礼申し上げます。

プロジェクトメンバー

本書は、独立行政法人情報処理推進機構　産業サイバーセキュリティセンター
中核人材育成プログラムにおける卒業プロジェクト
「セキュリティ投資を得る方法」の成果物として作成されました。

プロジェクトメンバー

上田　祐司
大塚　真緒
川上　理香
菊川　智史
椿　直樹
村上 由佳
藪田　樹
吉原　尚史

本書で使用しているアイコン、画像について

本書で使用している引用元の記載がないアイコン、画像は
以下のサイトのものを使用しています。

Unsplash
https://unsplash.com/ja

ICOOON MONO
https://icooon-mono.com/

iconmonstr
https://iconmonstr.com/