最近のサイバー攻撃手法と対策

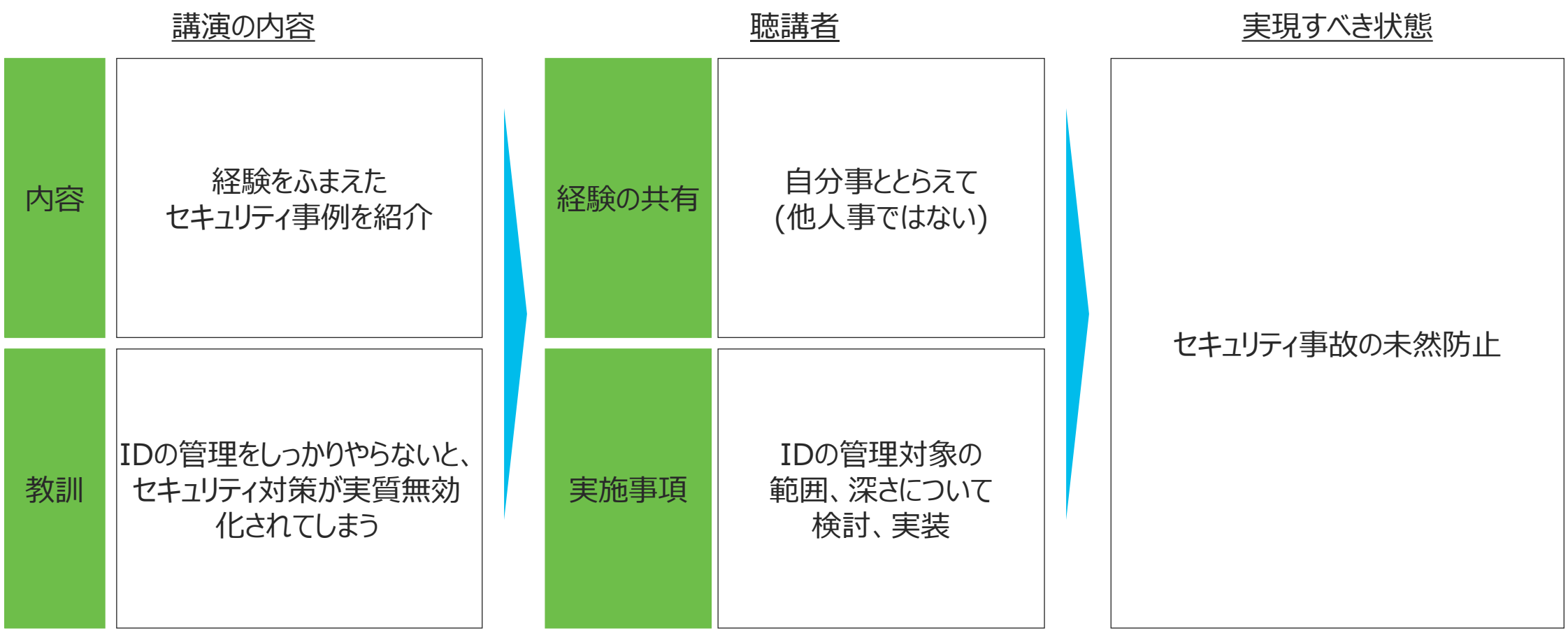
IDに対する攻撃について

加納　暢之

FutureWorks.Lab
CISCOセキュリティ事業アドバイザー
17/Apr./2025

本日の内容

過去の経験をふまえた事例を紹介します。本日はIDに関する内容です。
自分事ととらえてセキュリティ事故を未然に防止してください。



Agenda

- サイバーセキュリティの成熟度
- Talosが報告している最近のサイバー攻撃の傾向
- IDへのサイバー攻撃の手法
- IDへのサイバー攻撃に対する対策
- 最後に

サイバーセキュリティの成熟度

情報セキュリティ10大脅威とサイバー攻撃の被害の推移

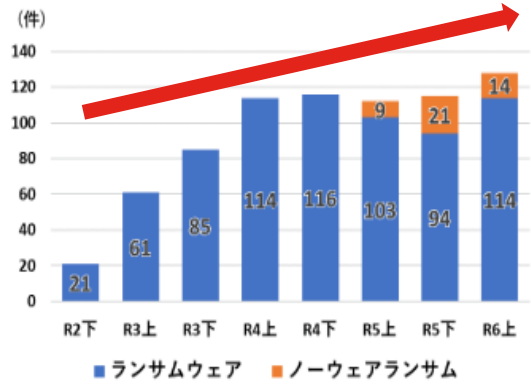
IPAの情報セキュリティ10大脅威[組織]※は、大きく変化していない。
一方、サイバー攻撃の被害は、発生し続けている。

	IPA 情報セキュリティ10大脅威[組織]	初選出年	10大脅威での取り扱い
1	ランサムウェアによる被害	2016	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019	6年連続6回目
3	内部不正による情報漏えい等の被害	2016	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016	9年連続9回目
5	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	2022	3年連続3回目
6	不注意による情報漏えい等の被害	2016	6年連続7回目
7	脆弱性情報の公開に伴う悪用増加	2016	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021	4年連続4回目
10	犯罪のビジネス化(アンダーグラウンドサービス)	2017	2年連続4回目

※2016年以降

被害の発生件数増加

(出典) 国立研究開発法人情報通信研究機構「NICTER観測レポート2023」を基に作成



なぜ、サイバー攻撃の被害が発生し続けるのか？
どこにリスクがあるのか？

最近の事例を紐解いてみましょう

出典:IPA情報セキュリティ10大脅威 2024
https://www.ipa.go.jp/security/10threats/10threats2024.html

出展:令和6年版 情報通信白書｜サイバーセキュリティ上の脅威の増大(総務省)
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/n21a0000.pdf

出展:令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について(警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

サイバー攻撃被害の事例

標的型攻撃(ランサムウェア)、DoS攻撃、IDに対する攻撃が報道されている。

標的型・ランサムウエアの例

KADOKAWA
KADOKAWA Group

トピックス

ランサムウェア攻撃による情報漏洩に関するお知らせ

株式会社KADOKAWA（本社：東京都千代田区、取締役 代表執行役社長 CEO：夏野剛）は、このたびの当社グループへのランサムウェア攻撃に起因した情報漏洩により、関係するすべての皆様に多大なるご心配とご迷惑をおかけしておりますことを深くお詫び申し上げます。

6月8日に当社グループの複数のサーバーにアクセスできない障害が発生した事実を受け、早急に社内で分析調査を実施したところ、ニコニコを中心としたサービス群を標的として、当社グループデータセンター内の株式会社ドワンゴ専用ファイルサーバーなどがランサムウェアを含む大規模なサイバー攻撃を受けたものと確認されました。

当社グループでは本事案発生時以降、社外の大手セキュリティ専門企業の支援を受けながら、情報漏洩の可能性および漏洩した情報の範囲を把握するための調査を鋭意進めてまいりました。このたび現時点の調査結果として、下記が判明しましたので、ご報告いたします。また、個人情報保護委員会に対しても、本内容を報告しております。

◆外部漏洩が発生したことを確認した情報

1. 個人情報　合計: 254,241人

【社外情報】

- 株式会社ドワンゴ関連の下記情報
- - 同社および同社の一部関係会社の一部取引先（クリエイター、個人事業主含む）の個人情報（氏名、生年月日、住所、電話番号、メールアドレス、活動名、口座情報など）
- - 年月日、住所、電話番号、メールアドレス、学歴・口座情報などの属性情報、社員番号・勤怠などの人事情報など）
- - 同社および同社の一部関係会社の面接を受けた一部の方の個人情報（氏名、生年月日、住所、電話番号、メールアドレス、選考履歴など）
- N中等部・N高等学校・S高等学校の在校生・卒業生・保護者・出願者・資料請求者のうち、一部の方々の個人情報（氏名、生年月日、住所、電話番号、メールアドレス、学歴などの属性情報、入学年・組・連絡先などの学生

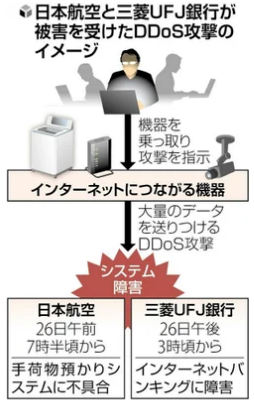
DoS/DDoSの例

10大脅威にない

ＪＡＬと三菱ＵＦＪ銀がサイバー攻撃被害…システム障害で警視庁が通信記録解析へ

2024/12/26 22:50　保存して後で読む

日本航空と三菱ＵＦＪ銀行は２６日、大量データ送付によるサイバー攻撃を受けたと発表した。両社ともに一時、システム障害が発生するなど利用者への影響が出た。日航から被害相談を受けた警視庁は、電子計算機損壊等業務妨害容疑を視野に、外部との通信記録を解析して発信元の特定を進める。



航空会社と銀行という重要インフラへの相次ぐ攻撃に政府は危機感を募らせている。大量にデータを送りつける「ＤＤｏＳ（ディードス）攻撃」とみられ、日航への攻撃について、政府は年末年始の繁忙期であることも踏まえ、旅客への対応を徹底するよう求めた。

日航によると、攻撃は２６日午前７時２４分に確認され、障害の起きたルーター（ネットワーク接続装置）を約１時間半後に一時遮断した。空港での手荷物預かりシステムの通信などで不具合が起きたが、関係するシステムは午後１時２０分に復旧。２６日午後８時現在、３０分以上の遅れは国内線６０便、国際線１１便の計７１便（最大４時間２分遅れ）で、４便が欠航した。安全上の支障はなかった。

IDの例

10大脅威にない

朝日新聞 ＞ 記事

電子カルテ、IDとPW使い回しでサイバー攻撃被害拡大 NEC構築

有料記事

編集委員・須藤龍也　2023年3月26日 5時00分

サイバー攻撃の被害に遭った大阪急性期・総合医療センター＝2022年10月31日午後7時33分、大阪市住吉区、飯塚悟撮影

NECが構築した電子カルテシステムを使う全国280の大規模病院のうち、半数以上の病院でサーバーやパソコンが病院ごとに同じIDとパスワードを使い回す状態になっていたことがわかった。 大阪市 の病院が昨秋に受けた サイバー攻撃 による被害の原因を調べる過程で、発覚した。NECは朝日新聞の取材に事実関係を認め、システムのセキュリティー対策を抜本的に見直すとしている。

使い回しで崩れた「閉域網神話」　NECを揺るがしたサイバー攻撃 →

サイバー攻撃の被害に遭ったのは、大阪急性期・総合医療センター（大阪市 住吉区 ）。

昨年10月、電子カルテのサーバーがランサムウェア（身代金ウイルス）に感染し、少なくとも数十台でデータが 暗号化 された。患者のデータなどが破壊され、約2カ月にわたって救急患者の受け入れや外来診療に影響が出た。

株式会社KADOKAWA
https://www.kadokawa.co.jp/topics/12088/

読売新聞　2024年12月26日
https://www.yomiuri.co.jp/national/20241226-OYT1T50207/

https://www.asahi.com/articles/ASR3T4VNZR3RULZU003.html

(仮説)サイバー攻撃対象・手法の変化

サイバー攻撃の手法は変化しつつある。標的型攻撃・ランサムウェアなどの攻撃手法が継続しつつも、
IDに対する攻撃など、危殆化しつつある企業インフラを攻撃する手法に回帰している。

サイバー攻撃の歴史的推移

		1990年代後半	2000年代初頭	2000年代後半～2010年代初頭	2010年代後半	2020年代初頭
攻撃手法の類型		アクティブ型の攻撃			パッシブ型の攻撃	アクティブ/パッシブ型の攻撃
攻撃手法		**① インフラへの攻撃(ホームページ改ざん/不正アクセス)**	**②ワーム**	**③DoS/DDoS攻撃(Webサイト)**	**④標的型攻撃ランサムウェア**	**④標的型攻撃ランサムウェア** **③DoS/DDoS攻撃(VPNなど)** **①インフラへの攻撃(ID)**
対策（例）	ポリシー(規定)		パッチマネジメント		ポリシーの整備(NIST CSF※など)	**危殆化するインフラを攻撃する手法に回帰**
	トレーニング				標的型メール訓練	
	ソリューション	FWの整備	端末にFW機能(OSの機能アップ)	CDNサービスの適用	SOCでの相関分析	**本日の話題**

※2014年２月　NIST：セキュリティフレームワーク制定　バージョン1.0

(仮説)サイバー攻撃対象・手法の変化の理由

セキュリティの強化に伴い、企業・組織の内部情報を窃取可能な、直接かつ安易な攻撃手法として、インフラ(ID)に対する攻撃に変化

攻撃者の状況	EDRの実装などに伴うセキュリティの強化により、マルウェアなどを用いて端末を感染させることが困難
企業・組織側の状況	在宅勤務などの増大に伴い、クラウドやVPNを利用して内部情報にアクセスさせるように業務のやり方に変化
ID運用の状況	クラウド(SaaS) → ID・パスワード認証だけで運用 企業内ネットワークのアクセス(VPN) → 休眠アカウントの存在
問題点	認証情報(ID・パスワード)を詐取されると、内部情報にアクセスできるようになってしまう
攻撃手法に変化	マルウェアなどを使用する必要がなく、直接攻撃が可能なインフラ(ID)に対する攻撃に変化

※企業のイントラシステムにおいても、内部犯行を防ぐ観点から、多要素認証は必要

(悪い例)CISCOのケース

CISCOにおけるサイバー事案。IDに対する攻撃(多要素認証疲労攻撃)によるもの。

https://gblogs.cisco.com/jp/2022/08/talos-recent-cyber-attack/

Cisco Japan Blog

Cisco Japan Blog / 脅威リサーチ / シスコに対する最近のサイバー攻撃についての Cisco Talos の洞察

2022年8月22日

Leave a Comment

脅威リサーチ

シスコに対する最近のサイバー攻撃についての Cisco Talos の洞察

2 min read

TALOS Japan

更新履歴

日付	更新内容
2022 年 8 月 10 日	Active Directory に関連したアクティビティについての詳しい説明を追加
2022 年 8 月 10 日	「シスコの対応と推奨事項」セクション（Duo 関連）を更新

概要

- 侵害を受けた可能性があることをシスコが認識したのは 2022 年 5 月 24 日です。以来、Cisco Security Incident Response（CSIRT）と Cisco Talos とで修復に取り組んでいます。
- 調査を進める中で、あるシスコ従業員のログイン情報が侵害されていたことが判明しました。侵害を受ける前に、この従業員の個人 Google アカウントを攻撃者が管理できる状態になっていたのですが、その個人アカウントではブラウザに保存されているログイン情報が同期される設定になっていました。
- 攻撃者は、この従業員に多要素認証（MFA）プッシュ通知を配信し、信頼できるさまざまな組織を装って一連の高度な音声フィッシング攻撃を仕掛け、通知を受け入れるように仕向けました。MFA プッシュ通知が受け入れられたことで、最終的に攻撃者は標的のユーザーのコンテキストで VPN にアクセスできるようになりました。
- 現在、CSIRT と Talos が対応にあたっていますが、製品開発やコード署名などに関連する重要な内部システムに攻撃者がアクセスしたことを示す証拠は確認されていません。
- 最初のアクセスを取得した後、アクセスを維持し、フォレンジック アーティファクトを最小限に抑え、環境内のシステムへのアクセスレベルを高めるために、攻撃者はさまざまなアクティビティを実行していました。
- この攻撃者は、環境から無事排除されました。攻撃後の数週間にわたり、粘り強くアクセスの回復を繰り返し試みていましたが、失敗に終わっています。
- 今回の攻撃は、UNC2447（サイバー犯罪グループ）、Lapsus$（攻撃者グループ）、Yanluowang（ランサムウェアを展開）とのつながりがある初期アクセスブローカー（IAB）としてすでに特定されている攻撃者によって実行されたと Talos では考えています（信頼性は中～高程度）。
- 詳細については、シスコの対応に関するこちらのページを参照してください。

個人アカウントの侵害から
Googleアカウントへのアクセス
Voiceフィッシング(Vishing)

MFA Fatigue(多要素認証疲労攻撃)

ユーザーの認証情報を入手した後、ボイスフィッシング（別名「ビッシング」"vishing"）やMFA疲労攻撃"MFA fatigue"※など、さまざまな手法を用いて多要素認証（MFA）をバイパスしようと試みる攻撃

※ MFA fatigue:誤って、あるいは単に繰り返し受信するプッシュ通知を黙らせるために、ユーザーが承諾するまでターゲットのモバイルデバイスに大量のプッシュ要求を送信するプロセス

生成AIでマルウェアを作成

生成AIを悪用し、マルウェアを作成することが可能。IDに対する攻撃も容易に可能。
サイバー攻撃の進化にあわせて、防御対象の拡大、作業の深化、高速化が必要。

生成ＡＩ悪用、知識なしでもウイルス作成…容疑の男「楽に稼ごうと」

2024/05/28 08:04 #生成ＡＩ 保存して後で読む

- フィッシングサイトへ誘導するメールの文面を作成
- 個人情報を盗む偽サイトを作成
- 爆発物や薬物の作り方を指南
- 詐欺事件への使用が懸念される、偽音声や動画を作成
- サイバー攻撃に使うウイルスのコードを作成

「楽に稼ぐため、コンピューターウイルスを作ろうとした」――。警視庁が２７日に不正指令電磁的記録作成容疑で逮捕した川崎市の無職の男（２５）はランサムウェアを作成しようとしたと供述しているという。対話型生成ＡＩ（人工知能）によるサービスが急速に広まる中で、繰り返し指摘されてきた犯罪に悪用される懸念が現実のものになった。

捜査関係者によると、男は元工場作業員で、ＩＴ会社への勤務歴やＩＴ技術を学んだ経歴はないという。これまでの捜査では協力者の存在も浮上していない。コンピューターに関する深い知識がない中で目を付けたのが、生成ＡＩの悪用だったとみられる。

[PR]

米オープンＡＩが「チャットＧＰＴ」の無料公開を始めたのは２０２２年１１月末だ。男はこの時期にニュースを見て生成ＡＩに関心を持つようになり、以前から興味があったというランサムウェアの作成を思いついたと説明しているという。

悪用されたのは「チャットＧＰＴ」などの大手サービスではなく、作成者が不明な状態でインターネット上に公開されていた複数の対話型ＡＩだったとみられる。警視庁は、男が自分のスマートフォンやパソコンから対話型ＡＩに質問を繰り返し、ウイルスを作成したとみており、男の自宅などから押収したパソコンやスマホを解析し、事件の全容解明を急いでいる。

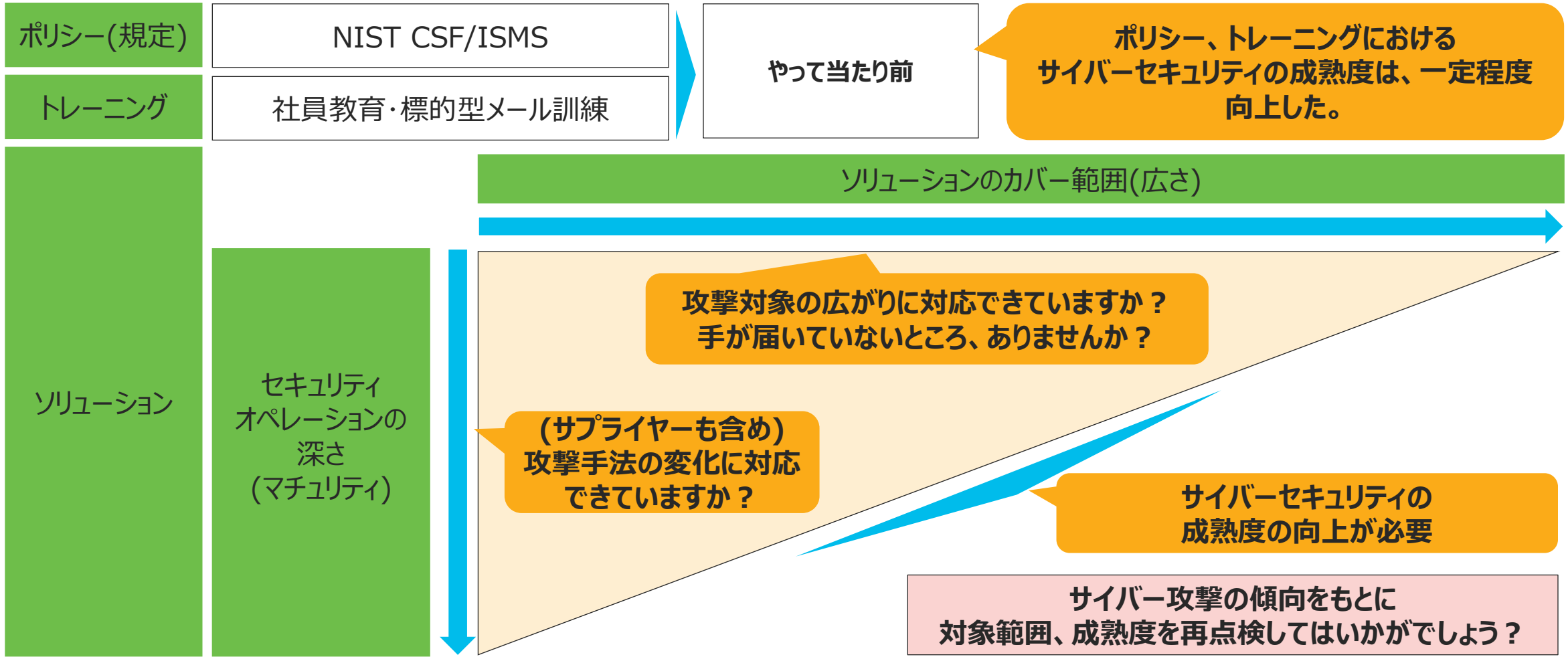
https://www.yomiuri.co.jp/national/20240528-OYT1T50021/

今後の予測

	サイバー攻撃	防御
対象範囲	拡大	拡大
作業	自動化、深化、高速化	自動化、深化、高速化

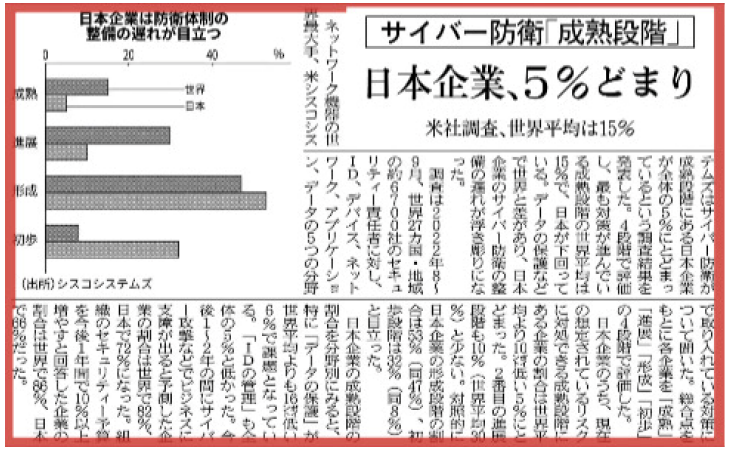
サイバーセキュリティの成熟度

NIST CSFなどの網羅的なポリシーに基づき、標的型攻撃に対するポリシー整備、トレーニングが一般化。
一方、攻撃対象、手法は変化、危殆化したソリューションの再チェック、オペレーションの成熟度の向上が必要。



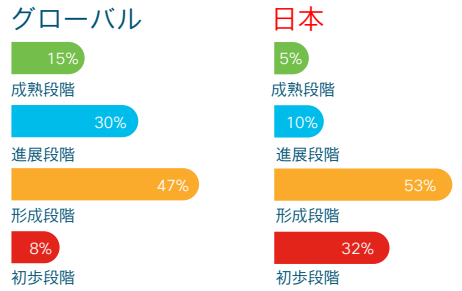
日本企業のサイバーセキュリティの成熟度

シスコの調査によれば、日本企業のサイバー防衛における成熟度は諸外国に比較し低い。



Source:
https://www.nikkei.com/article/DGXZQOUC222450S3A320C2000000/

「シスコ サイバーセキュリティ成熟度指標」の調査結果



Source: https://www.cisco.com/c/dam/m/ja_jp/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-market-snapshot-japan.pdf

72% 今後 12～24ヵ月間にサイバーセキュリティのインシデントによりビジネスに支障をきたすと予測した日本企業の回答者

66% サイバーセキュリティ予算を今後12ヵ月で最低 10%増やす予定と回答した日本企業

成熟度（マチュリティ）を上げていきましょう

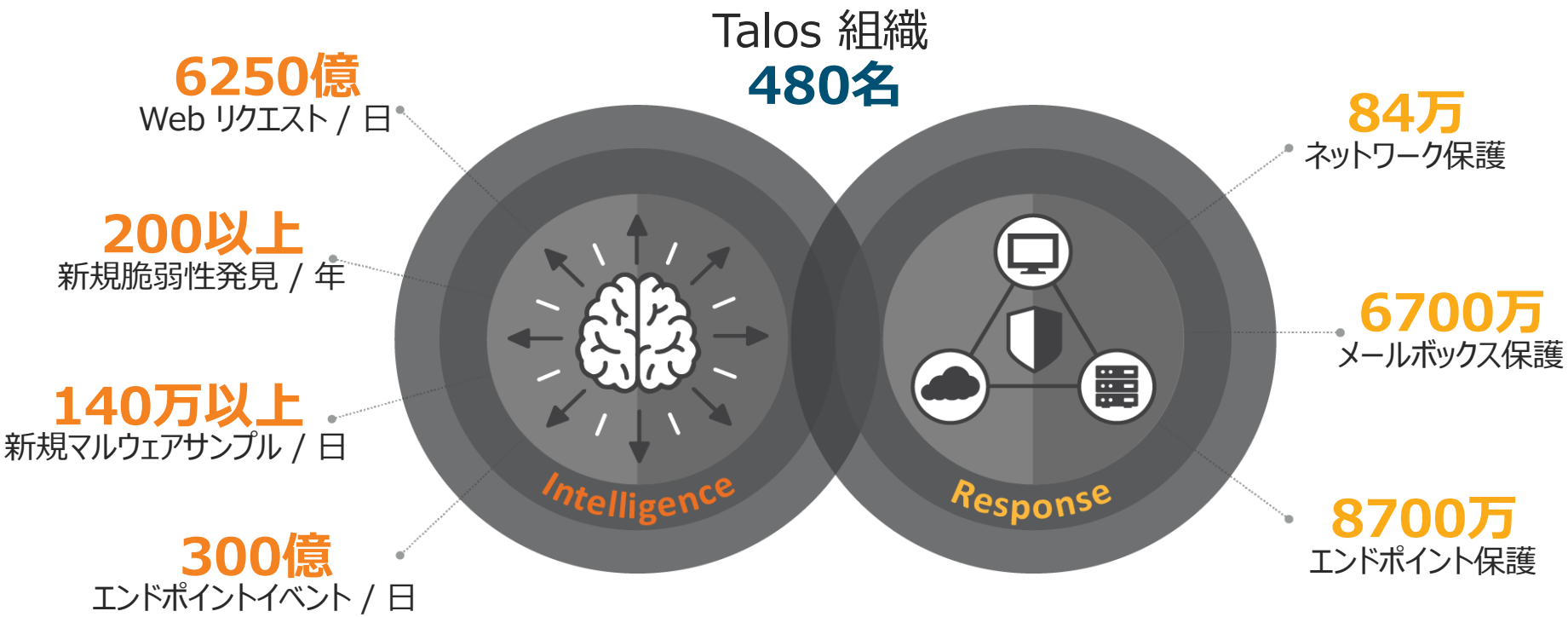
2023年サイバーセキュリティの現在地
日経新聞：「日本企業のサイバー防衛、「成熟」は5%　シスコ調査」

Talosが報告している最近のサイバー攻撃の傾向

Talosとは？

CISCOのサイバーセキュリティに係るインテリジェンスチーム

- 悪意ある行為から、お客様やユーザを守るために情報収集、分析、配布
- Talosは、情報の質、量ともに世界トップクラスの評価



※数字は2024年末時点の概数

Talosの活動の紹介

Talosは、多くのチャネルを通じてセキュリティ情報をタイムリーに公開、インターネットがより安全なものになるように支援。

ホワイトペーパー, 記事 & 関連情報
talosintelligence.com

脅威情報 ニュースレター
cs.co/TalosUpdate

Talos ブログ
blog.talosintelligence.com

ソーシャルメディアへのポスト
x.com/talossecurity

インストラクションビデオ
cs.co/talostube

Beers with Talos & Talos Takes
talosintelligence.com/podcasts

Talosで検知している脅威

Talosの情報では、以下の攻撃手法が報告されている。

1	Webアプリケーションの脆弱性 / Web shells
2	ランサムウェア
3	標的型攻撃
4	クラウドアプリケーションに対する攻撃 / Initial Access

サイバー攻撃対象・手法の変化
(IPAの10大脅威にないところ)

有効なアカウント(ID)に対する攻撃 / Valid accounts

https://blog.talosintelligence.com/category/ctir-trends/

Talos IS Q1 2024(January-March)
https://blog.talosintelligence.com/talos-ir-trends-q4-2024/

IDに対するサイバー攻撃の状況(Talosの報告)

IDに対するサイバー攻撃は、他のサイバー攻撃に比較して簡単かつ効果が大きいことから増加傾向にある。
最近のIDに対するサイバー攻撃の手法は、大きく４種類ある。

#	IDに対して脅威の状況	原因・理由
1	アイデンティティベースの攻撃は増加傾向	非常に効果的
2	初期アクセス経路のトップは過去に侵害されたIDの使用	有効(真正)なアカウントの認証情報を利用することにより侵害されていることの検知が困難
3	上位の弱点は、脆弱であるか、設定が間違っていた	システムとMFAの欠如

#	IDへのサイバー攻撃の手法
1	パスワードスプレー攻撃 Password spraying
2	クレデンシャルハーベスティング Credential harvesting featured in a fourth of incidents
3	AiTM フィッシング Adversary-in-the-middle (AiTM) phishing
4	内部犯行 Insider threats

IDの攻撃について、例示

IDへのサイバー攻撃の手法

IDへのサイバー攻撃の手法

パスワードスプレー攻撃

パスワードスプレー攻撃

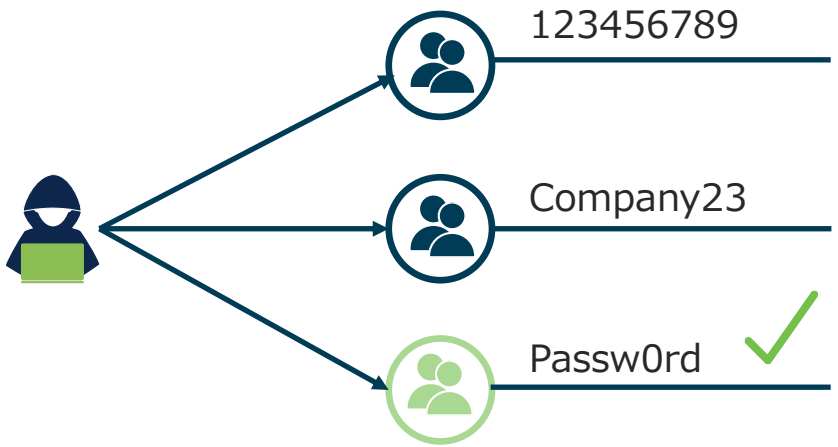
多数のアカウントに対して同一のパスワードリストを用いて、ログインを試みるサイバー攻撃

- 大きくは、ブルートフォース攻撃の一形態
- 多くのアカウントに対して、少数のパスワードを試行するため、不正なログイン試行の検知が困難
- アカウントを乗っ取られ、不正利用されたり、情報を窃取される。

✓ **パスワードスプレー攻撃**

Brute Force: Password Spraying [T1110.003]

多数のアカウントに少数の一般的なパスワードを順番に試す



IDへのサイバー攻撃の手法

クレデンシャルハーベスティング攻撃

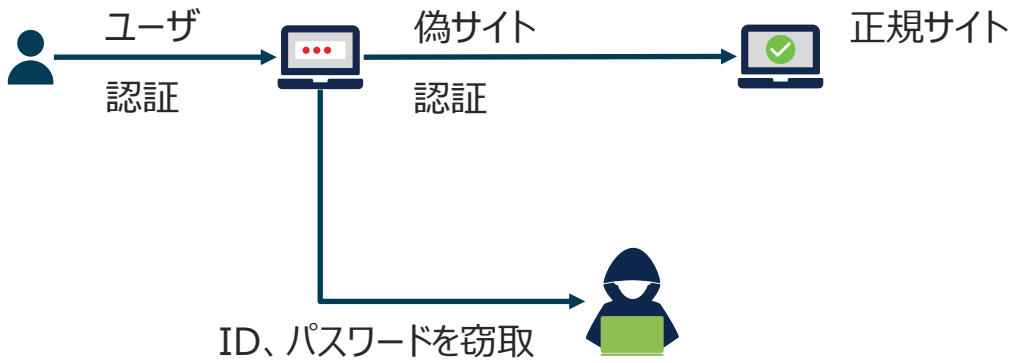
クレデンシャルハーベスティング攻撃

攻撃者が、秘密裏にユーザ名、パスワードなどのクレデンシャル情報を秘密裏に収集すること

- フィッシングメール、マルウェアを用いたもの、中間者攻撃などを用いたものなどがある。

✓ **クレデンシャルハーベスティング攻撃**
Credential Harvesting[TA0006]

偽サイトでID、パスワードを窃取



IDへのサイバー攻撃の手法

AiTM フィッシング攻撃

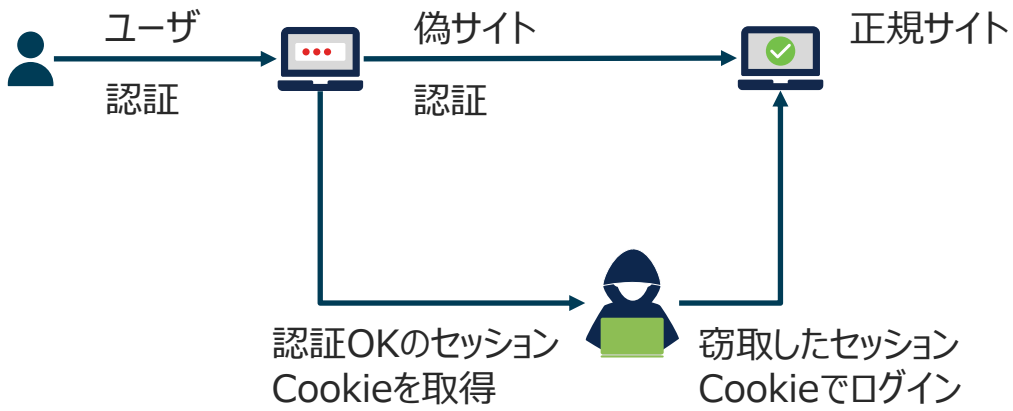
AiTM フィッシング攻撃とは

ターゲットのパスワードと Web サイトとの間のセッション情報の窃取を目的としたフィッシング攻撃。

- Web サイト（攻撃者が偽装したいサイト）の間にプロキシサーバーを配置し、セッション情報を窃取

✓ **AiTMフィッシング攻撃**
Adversary-in-the-Middle [T1557]

通信傍受で盗んだセッションCookieでログイン



IDへのサイバー攻撃の手法

内部犯行(内部不正)

内部犯行(内部不正)とは

企業の従業員や関係者などの内部者が犯罪もしくは犯罪に類する行為を行うこと。
内部犯行には、３要素があり、対策として大きく４つ。

技術的対策は、内部犯行の機会を減らすために重要。
標的型攻撃などにおけるラテラルムーブメント対策やITサプライチェーン対策としても有効。

#	内部犯行の3要素
1	動機
2	機会
3	正当化

内部犯行の対策

- 罰則
- 規則の制定
- 教育の実施
- 技術的対策

感染した端末の振る舞い(ラテラルムーブメント)は、内部犯行における振る舞いと変わらない。

技術的対策は、機会を減らすために重要
≒ラテラルムーブメント/ITサプライチェーン対策と共通

参考：内部不正を防止するための企業・組織の体制の現状　調査結果
https://note.com/ipasecuecono/n/n287b5649c401

ITサプライチェーン

サプライチェーンの脅威シナリオとしてIPAの実態調査から大きく2つの類型がされている。
平昌では、類型①のITサプライチェーンで侵入されている。

サプライチェーン			脅威シナリオ例		例
類型①	ITサプライチェーン	委託先でのサイバーセキュリティインシデント	委託元のシステム・サービスの障害、情報漏洩、データ毀損	システム・サービスの障害	平昌
類型②	ソフトウェアサプライチェーン	開発・製造・流通・配布などのサプライチェーンの過程においてマルウェアを混入	ソフトウェア製品やハードウェア製品内のソフトウェア(ファームウェア)	マルウェアの混入	-

【参考】IPA:ITサプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査
https://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_1/pdf/002_s03_00.pdf

【参考】IPA:サプライチェーンにおけるサイバーセキュリティ対策の強化について
https://www.ipa.go.jp/security/sc3/news/20220331.html

内部犯行の対策

感染した端末の振る舞い(ラテラルムーブメント)は、内部犯行における振る舞いと変わらない。
IDの管理(Step1)、次にラテラルムーブメント対策/ITサプライチェーン対策(Step2)が必要。

Step1	ID管理	IDの管理が適切に行われていないと、セキュリティデバイスの機能が実質無効化される

	#	一般的な内部犯行対策	細部説明
Step2	1	外部記憶装置の使用制限	USBメモリや外部ハードディスクなどの使用を制限し、社内ルールによる、持ち出し対策
	2	アクセス制限	重要な情報へのアクセス権限を最小限にし、定期的に見直すことが必要
	3	退職者のID削除	退職者のIDやアクセス権限を迅速に削除し、遠隔操作ソフトのインストールなどをチェック
	4	アクセスログの取得と管理	重要データへのアクセスログを取得し、定期的に監視
	5	監視カメラの設置	重要データを扱う場所や部屋に監視カメラを設置し、入退室管理システムを導入
	6	研修の実施	従業員に対して情報セキュリティやコンプライアンスに関する研修
	7	罰則規定の設定	内部犯行に対する明確な罰則規定を設け、厳しく適用

IDへのサイバー攻撃の手法

その他　IoT機器に対する攻撃

IoT機器に対する攻撃

IoT機器のセキュリティ対策実施していますか？
総務省からは、IoT機器を悪用した攻撃が増加しているとの広報。

IoT機器の例

サイバー攻撃に悪用されるおそれのあるIoT機器の調査（NOTICE）の取組強化

―国立研究開発法人情報通信研究機構法附則第8条第2項に規定する業務の実施に関する計画の変更の認可―

総務省は、国立研究開発法人情報通信研究機構（理事長：徳田 英幸）から申請があった国立研究開発法人情報通信研究機構法附則第8条第2項に規定する業務（NOTICE）の実施に関する計画の変更について、本日認可をしましたので、公表いたします。

1 背景

近年、IoT機器を悪用したサイバー攻撃が増加していることから、利用者自身が適切なセキュリティ対策を講じることが必要です。

こうした状況を踏まえ、国立研究開発法人情報通信研究機構法（以下「法」といいます。）の改正が平成30年11月に行われ、国立研究開発法人情報通信研究機構（NICT）の業務（法附則第8条第2項に規定する業務）として、サイバー攻撃に悪用されるおそれのある機器の調査等を行うこととなっています。当該業務に当たっては、法の規定に基づき、当該業務の実施に関する計画をNICTが定め、総務大臣の認可を受けることとなっており、総務省は、平成31年1月25日に当該計画の認可を行っています。

上記手続きを踏まえ、NICTでは、平成31年2月20日からインターネット上のIoT機器に、容易に推測されるID・パスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報をインターネット・サービス・プロバイダ（ISP）へ通知しています。ISPでは、当該通知を受け、該当する機器の利用者を特定し、注意喚起を実施しています。（別紙参考）

https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00079.html

適切に管理されていないIoT機器がサイバー攻撃(DoS攻撃)の温床

IoT機器のID管理やってますか？

IDへの攻撃に対する対策

IDへの攻撃への対策

パスワードスプレーなど、IDへの攻撃への対策は、概ね共通の対策となる。

#	IDへの攻撃への対策	広さ(対象範囲)：例	深さ(成熟度) ：例	ソリューション例
1	ID管理	全ての機器のIDは管理されていますか？	不要なIDありませんか？ 定期的に棚卸していますか？	Duo
2	トレーニング	IDの内容は含まれてますか？	IDへの攻撃対策についてトレーニングしていますか？	-
3	多要素認証	オンプレミスのサーバにも適用されていますか？	パスワードレスに移行しませんか？	Duo
4	監視	クラウドのサービスの監視していますか？	パスワードスプレーの監視できていますか？	XDR Splunk
5	脆弱性対策・パッチマネジメント	ネットワーク機器/IoT機器への脆弱性対策やってますか？	ネットワーク機器/IoT機器へのパッチマネジメントの周期はどのくらいですか？	Vulnerability Management
6	インシデントレスポンス	IDの対応はありますか？	パスワードの変更など、IDの対応を実際にやっていますか？	XDR Splunk

IDの管理、監視、インシデントレスポンスについて説明

ID管理

ID管理も資産管理の一つなので、適切に管理していただきたいと思います。
NIST CSFでもID.AM-01と、資産が管理されているかを問うています。

機能領域	カテゴリ	カテゴリ
ガバナンス(GV)		
識別(ID)	ID.AM	資産管理
防御(PR)	PR.AA	資産へのアクセス
検知(DE)	⋮	⋮
対応(RS)		
復旧(RC)		

資産管理は、セキュリティの一丁目一番地

IDを管理することも、資産管理の一部

IDの管理も、範囲(網羅性)と深さ(成熟度)を上げましょう。

休眠アカウントありませんか？

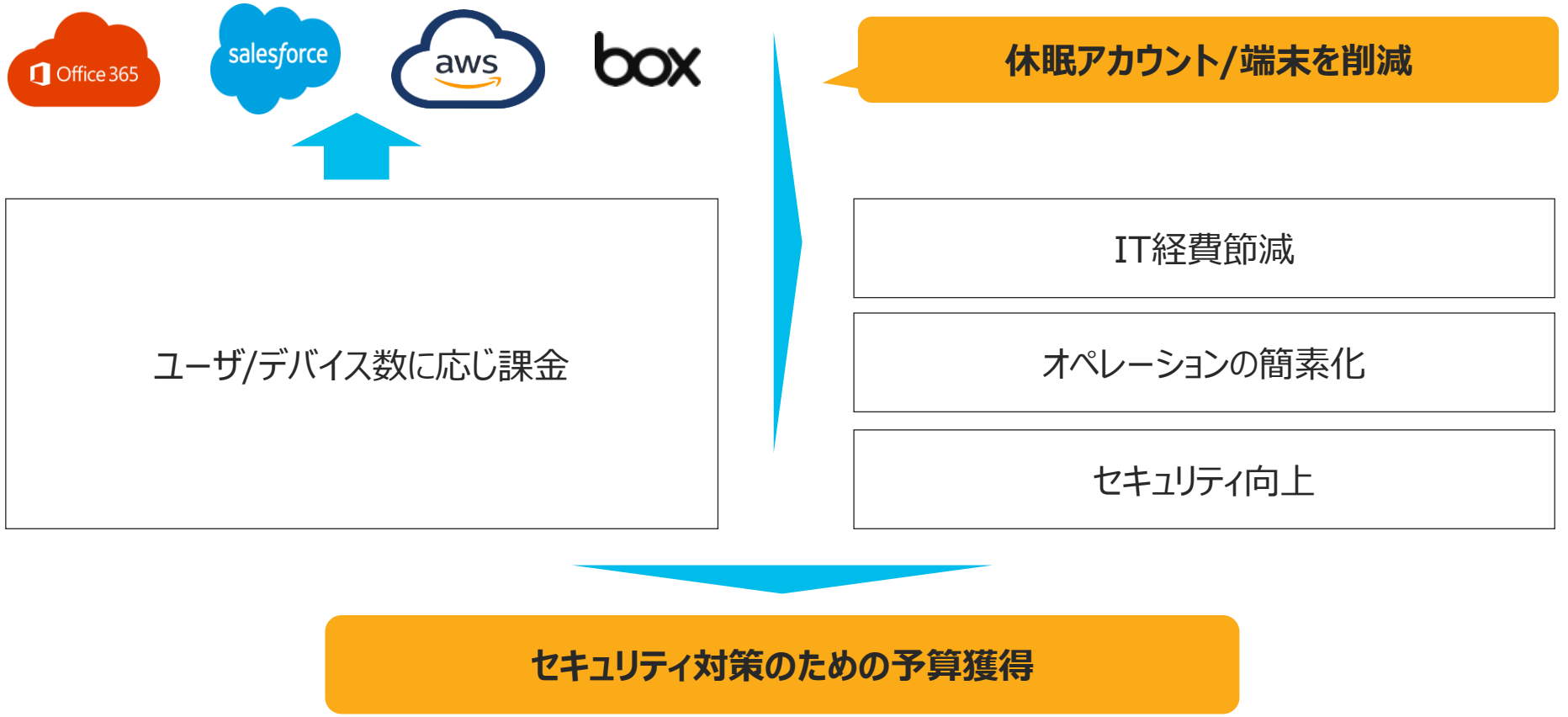
IDに関するLogを取得していますか？

多要素認証実施していますか？

ID管理の深化による予算の節減とセキュリティ対策の向上

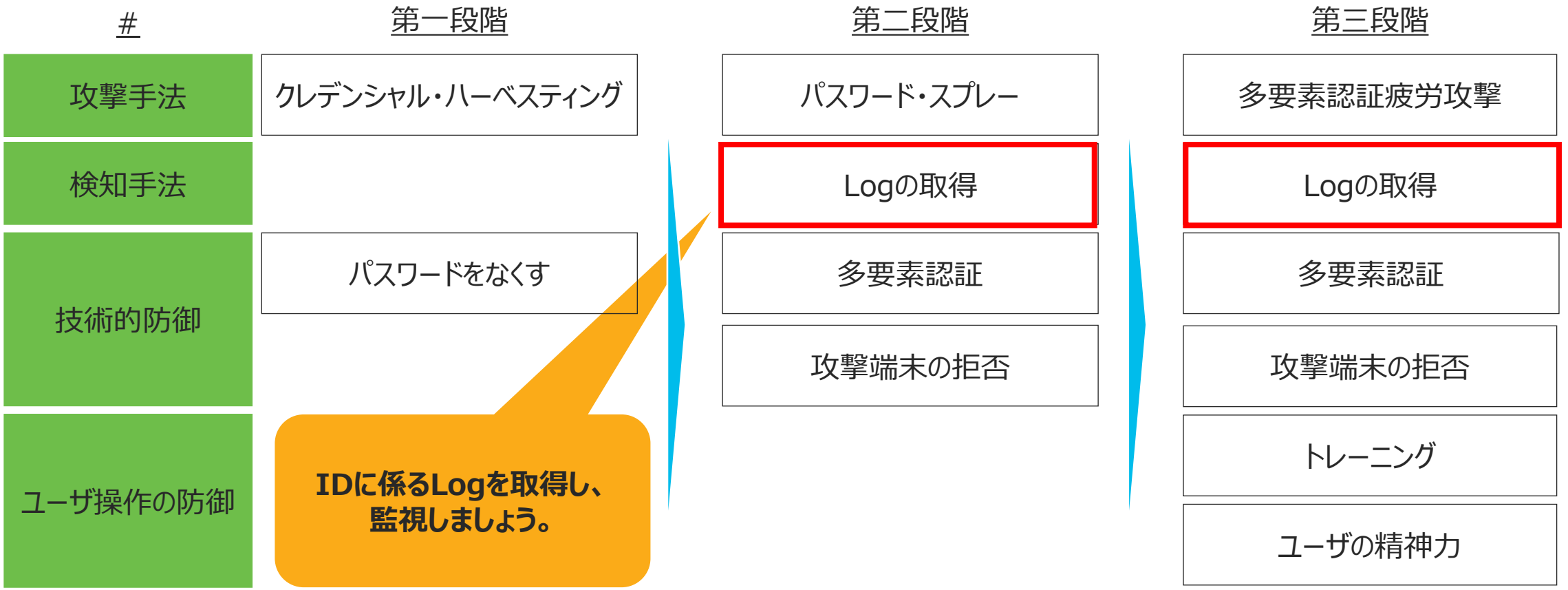
IDの管理を適切に行うことで、IDに連携したクラウドサービスの価格を節減することが簡単に可能です。

定期的に休眠アカウントを発見、IT経費を節減し、サイバーセキュリティ対策を向上していくことをお勧めします。



監視

IDの作成、削除、使用状況を監視していなければ、攻撃を受けている兆候すら認識できません。IDの使用状況について監視するようにしましょう。



インシデントレスポンス

多要素認証疲労攻撃の段階になると、ユーザは通常の業務にならなくなるので、拒否し続けることは精神的に困難に陥ります。手前の段階で、攻撃者を排除するオペレーションを構築しておきましょう。

#	第一段階	第二段階	第三段階
攻撃手法	クレデンシャル・ハーベスティング	パスワード・スプレー	多要素認証疲労攻撃
検知手法		Logの取得	Logの取得
技術的防御	パスワードをなくす	多要素認証 攻撃端末の拒否	多要素認証 攻撃端末の拒否
ユーザ操作の防御			トレーニング ユーザの精神力

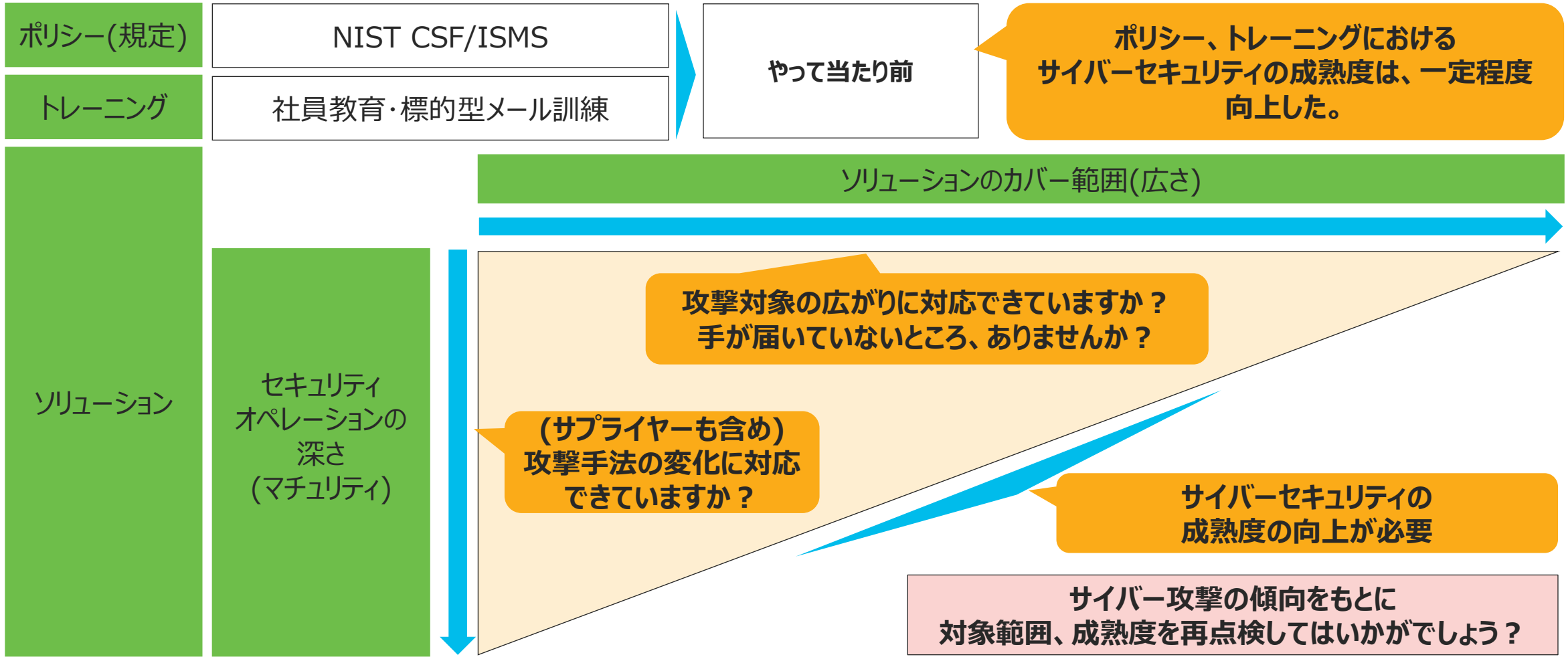
ユーザの精神力に頼る前に、技術的対策をとりましょう。

最後に

サイバーセキュリティの成熟度

再掲

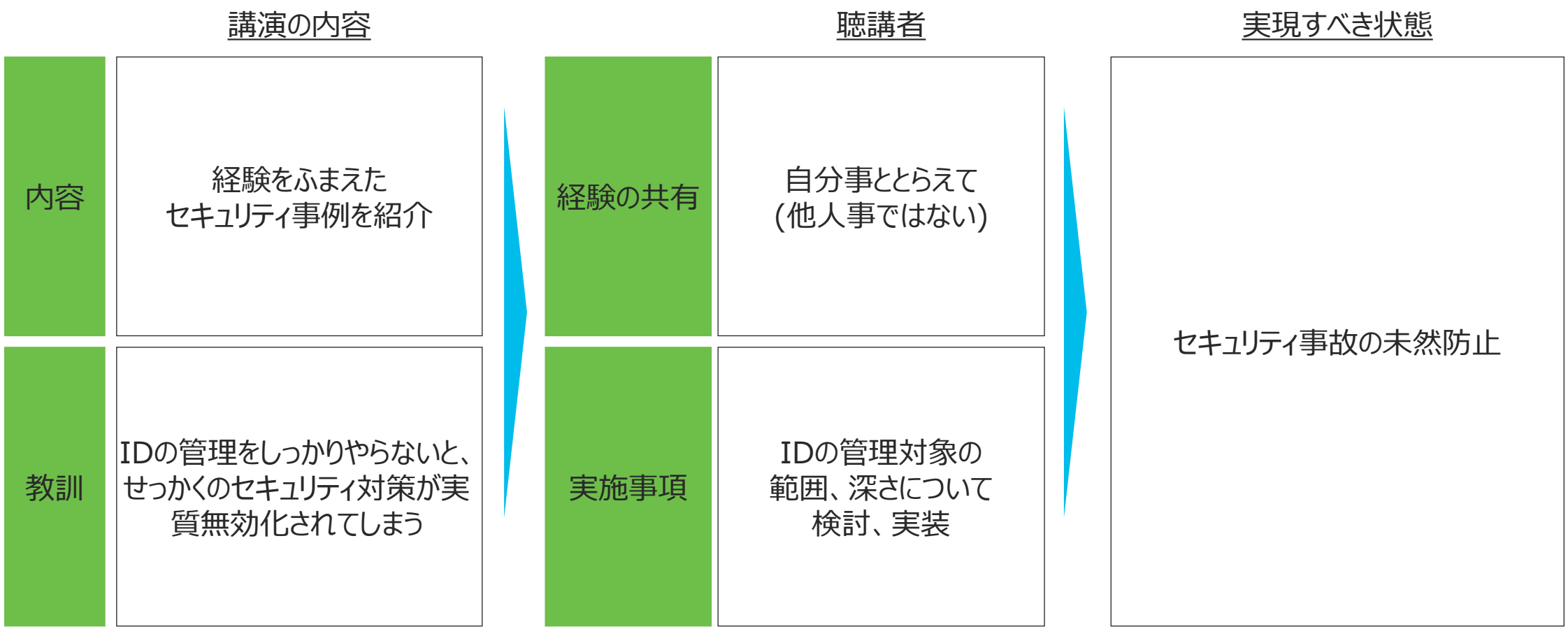
NIST CSFなどの網羅的なポリシーに基づき、ポリシー整備、トレーニングが一般化しつつある。一方、攻撃対象、手法は変化、危殆化したソリューションの再チェック、オペレーションの成熟度の向上が必要。



本日の内容

再掲

本日はIDに関するセキュリティ事例について紹介。
自分事ととらえてセキュリティ事故を未然に防止してください。



End