第9日午前1

製造業ITマイスター指導者育成プログラム
研修テキスト　講義用教材（第９日）
情報システムセキュリティ基礎

製造業ITマイスター研修教材一覧

日	テーマ		教材
1	製造業IT導入ワークショップ	午前	IoTとシステムの基礎
		午後	製造業IT導入ワークショップ
2	高度IT実装技術の習得１	午前	IoTによるシステム開発入門
		午後	高度IT実装技術の習得１（ラズパイ＋見える化実習）
3	高度IT実装技術の習得２	午前	IoTによる生産管理入門
		午後	高度IT実装技術の習得２（IoTセンサー実装実習）
4	システム構築技術の習得１	午前	IoTによる在庫管理入門
		午後	システム構築技術の習得１（業務システムの基本パターン）
5	システム構築技術の習得２	午前	IoTによるデータ分析入門
		午後	システム構築技術の習得２（データ分析）
6	PBL１（事例企業調査）	午前	事例企業調査
		午前	事例企業の課題モデル化実習
7	PBL２ （課題の設定と解決策の提案）	午後	システム構築の実際
		午後	システム構築実習（１）課題の設定と解決策の提案
8	高度ＩＴ実装技術の適用	午前	IT経営の実践方法
		午後	システム構築実習（２）高度ＩＴ実装技術の適用
9	システム構築技術の適用	午前	情報システムセキュリティ基礎
			知財とオープン＆クローズ戦略
		午後	システム構築実習（３）システム構築技術の適用
10	筆記試験および成果発表会	午前	個人と組織の発展に繋がるキャリアデザイン講座
			（筆記試験）
		午後	（成果発表会）

もくじ

1. 情報システムセキュリティの現状と課題

2. IoT機器関連のセキュリティ脅威と課題

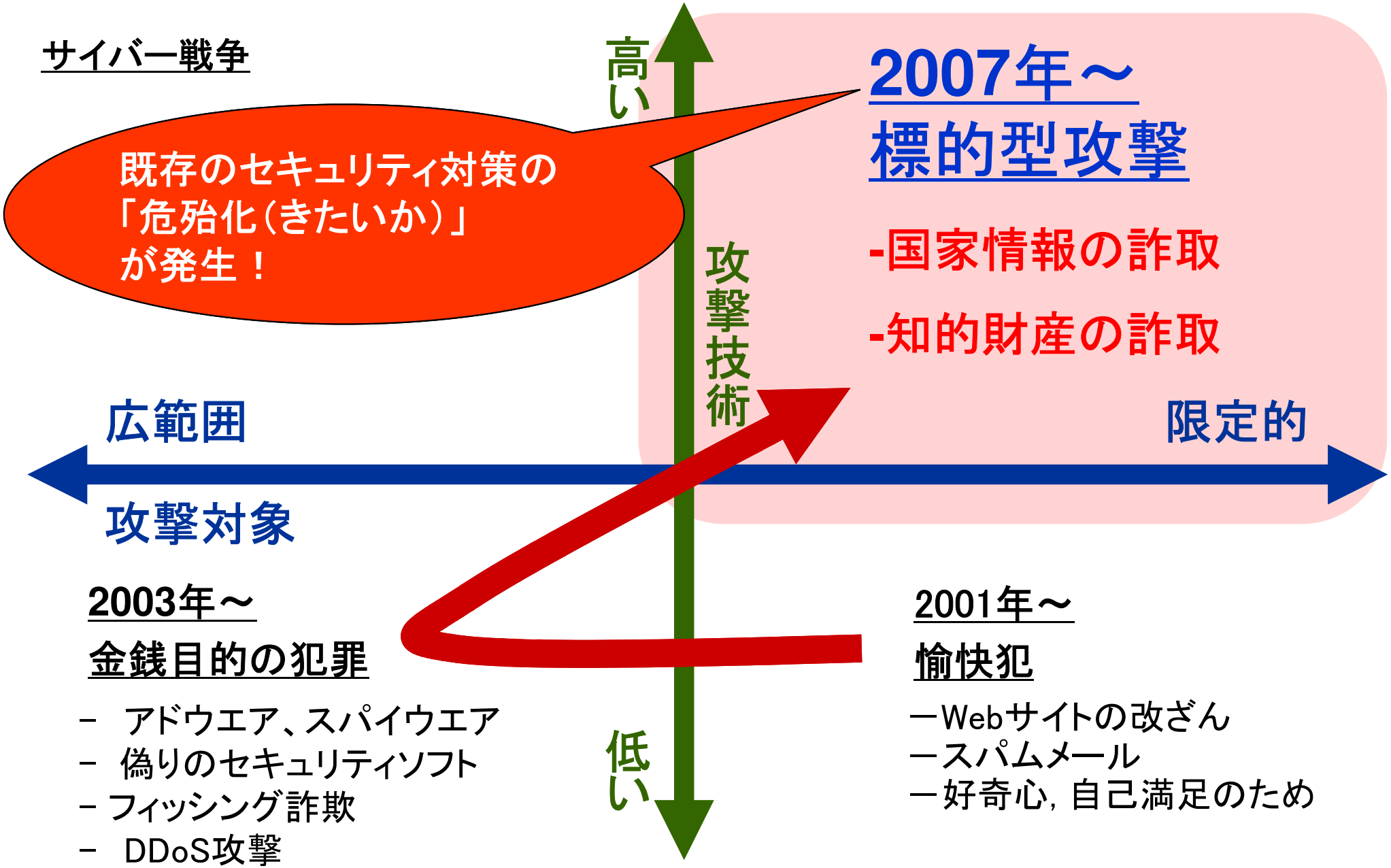
3. IoT関連セキュリティのトピックスと対策

情報セキュリティ10 大脅威 2019

昨年順位	個人	順位	組織	昨年順位
1位	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者への被害	3位	ランサムウェアによる被害	2位
NEW	メール等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

出典：情報処理推進機構「情報セキュリティ10大脅威2019」
https://www.ipa.go.jp/files/000071831.pdf

サイバー犯罪の分類と歴史的変遷



サイバーセキュリティへの脅威の実態

国内事例

2015年5月：**日本年金機構**の職員が利用する端末がマルウェアに感染し、年金加入者に関する情報約125万件が流出（**標的型攻撃**）

2015年10月：**金融庁**の注意喚起を装ったフィッシングサイトを確認、国内銀行のセキュリティを向上させるためと称し、口座番号、パスワード、第二認証などの情報を騙し取られる恐れ（**フィッシング攻撃**）

2015年11月：**東京五輪組織委員会**のホームページにサイバー攻撃、約12時間閲覧不能（**DDoS攻撃**）

2016年6月：**i.JTB（JTBのグループ会社）**の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（**標的型攻撃**）

2017年5月：国内（行政、民間企業、病院等）において、**WannaCry**による被害が確認。企業内のシステム停止などの障害が発生した。（**ランサムウェア**）

海外事例

2015年4月：**フランスのテレビネットワークTV5Monde**がサイバー攻撃を受け、放送が一時中断（**標的型攻撃**）

2015年6月：**米国の人事管理局（OPM）**が不正にアクセスされ、政府職員の個人情報が流出（**不正アクセス**）

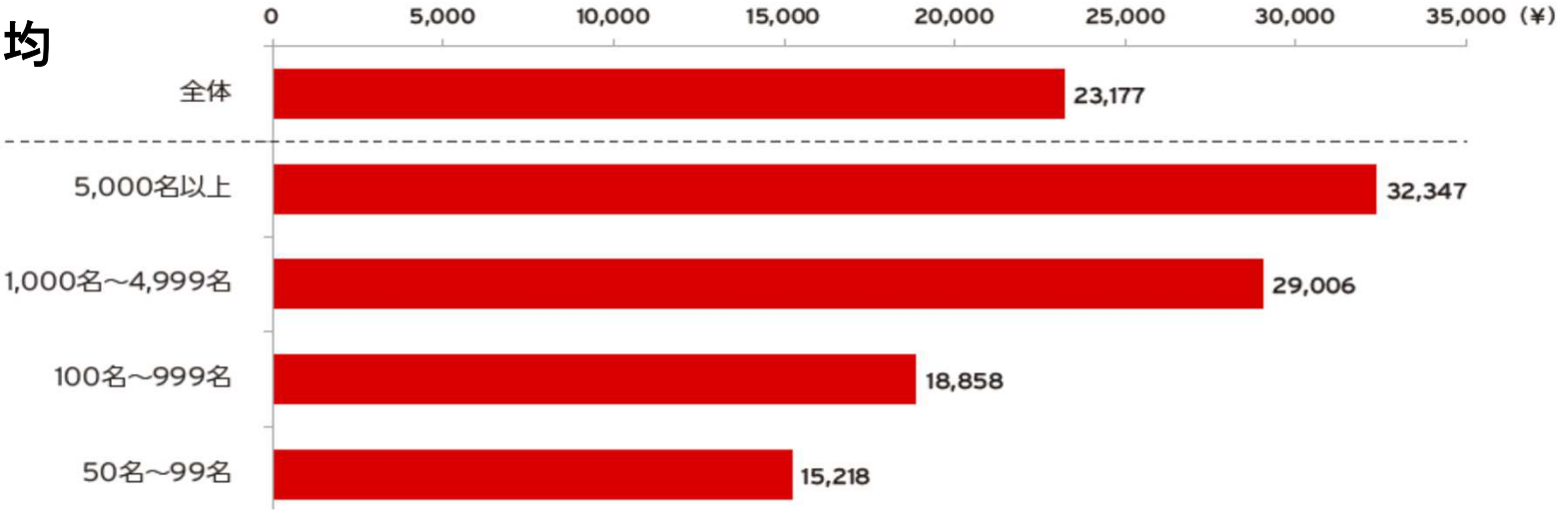
2015年12月：**ウクライナの電力会社**のシステムがマルウェアに感染し、停電が発生（**標的型攻撃**）

2016年10月：**米国のDyn社**のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（**DDoS攻撃**）

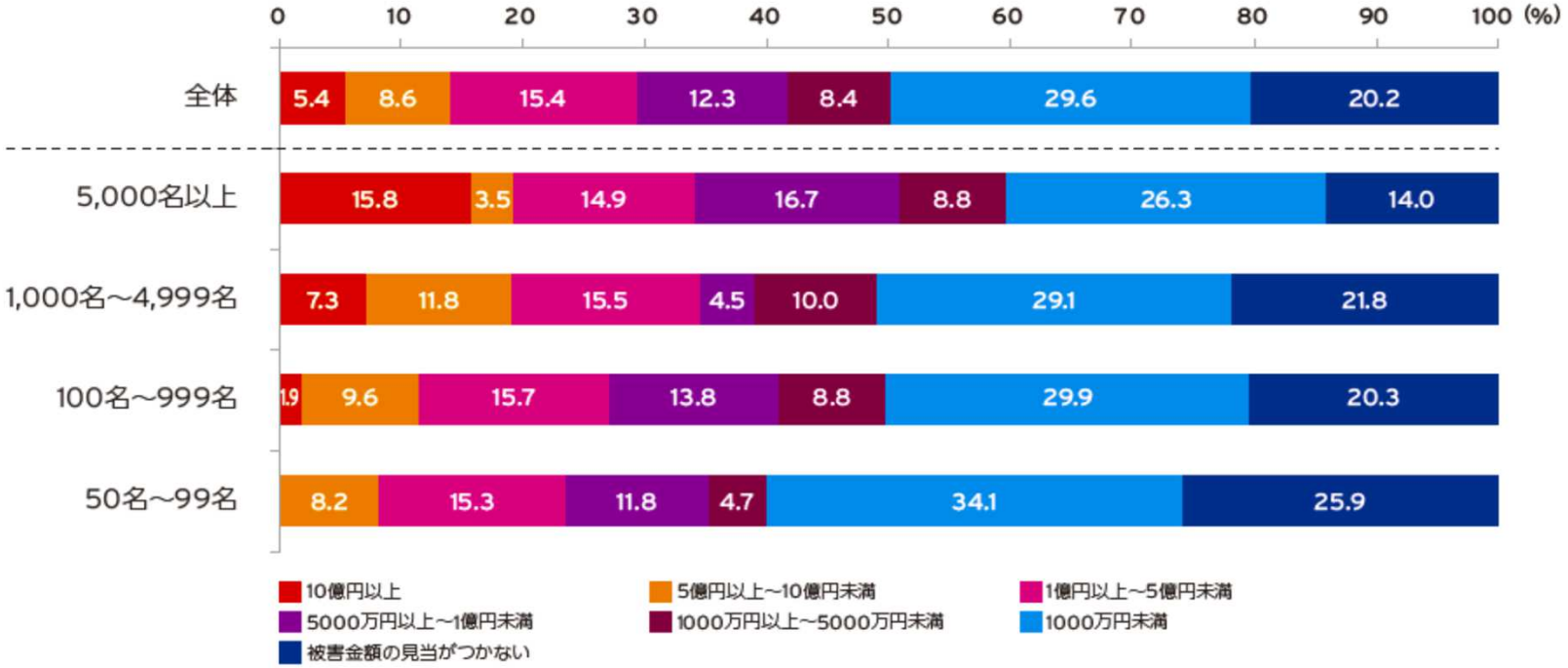
2017年5月：世界各国（アメリカ、イギリス、中国、ロシア等）で**WannaCry**の感染被害が発生。行政、民間企業、医療等の多くの組織に影響を及ぼした。（**ランサムウェア**）

重大被害による年間被害金額

年間被害総額平均（規模別）



年間被害総額内訳（規模別）



法人組織におけるセキュリティ実態調査（トレンドマイクロホワイトペーパー2017年版）

情報漏洩の企業へのインパクト

「情報漏洩事故が起こると通常、**以下の費用が発生**する。

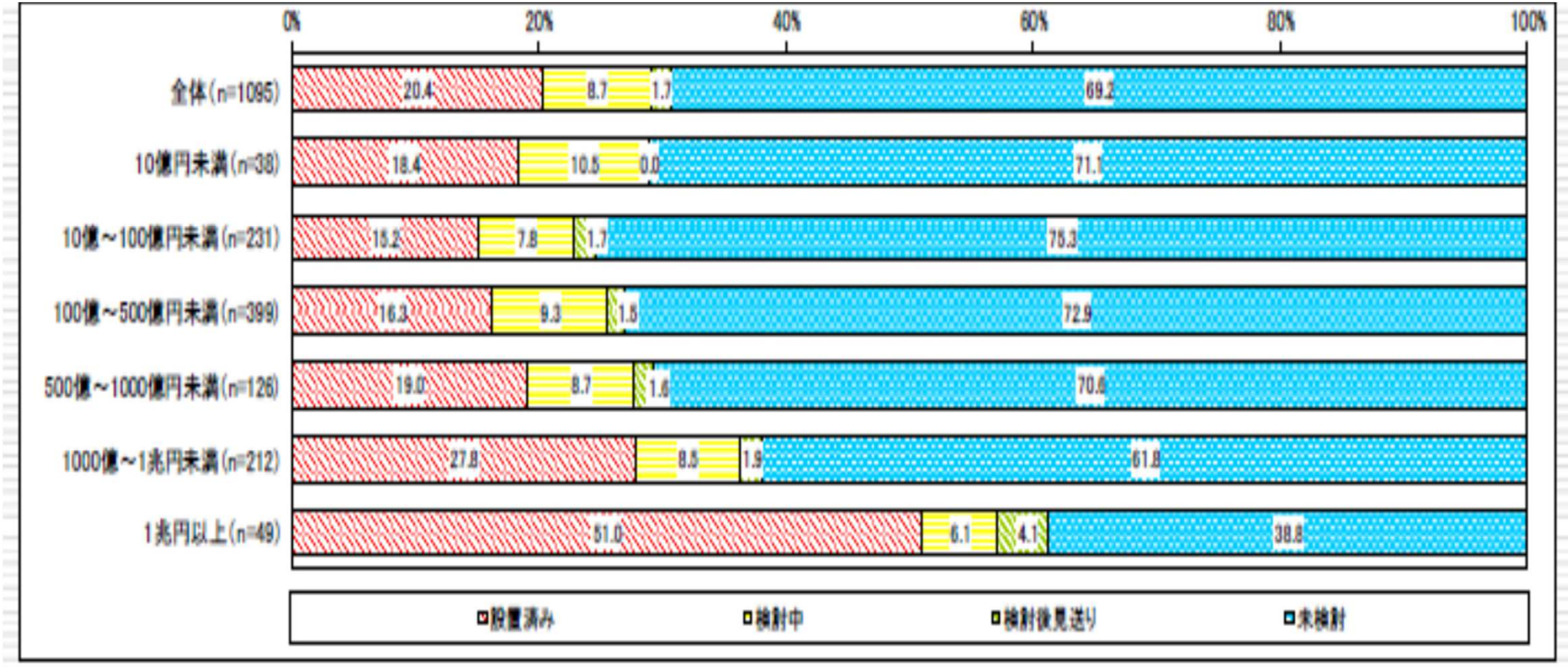
1. 謝罪広告の掲載
2. 会見の設定
3. おわび状の作成・送付
4. 顧客への補償
5. 顧客対応コールセンターの設置
6. 応急処置のためのシステム改修
7. 原因究明と本格的な対策の実施
8. セキュリティー専門家などコンサルティングの実施
9. サイトなどの停止期間の売り上げ機会損失
10. 社会的信用失墜や企業イメージの低下に伴う経営上の損失
11. 株価の下落による資産の減少
12. 民事訴訟で敗訴した場合の損害賠償 など

最悪1,000億円規模になると言われている。」

2011年8月8日　日本経済新聞　佐々木良一 教授
東京電機大学大学院 未来科学研究科 情報メディア学専攻 情報セキュリティ研究室

売上高別CISOの設置状況

- 企業規模が大きいほど専任のCISO(*)を置くなど
  セキュリティ意識は高く、経営幹部の関わりも深い。



CISO：Chief Information Security Officer（最高情報セキュリティ責任者）

一般社団法人日本情報システム・ユーザー協会「企業IT動向調査2019」

大きな勘違い「ウチの会社なんて」

ウチのデータなんて盗まれたって困らないね。カネを掛けて守る価値なんてないよ！

メッセージ①
ハッカーは売上高や従業員数などで攻撃先を選んでいる訳ではありません！
（IPアドレスによる全数攻撃）

メッセージ②
最初は「被害者」でも途中からは「加害者」の一味にされてしまいます！

被害者

ハッカーによるデータ漏洩、システム乗っ取り

ゾンビ（ボットネット）の仲間入り！

加害者

ハッカーが貴社のシステムを攻撃メンバーに追加

ハッカーの他社への攻撃に貴社が加担

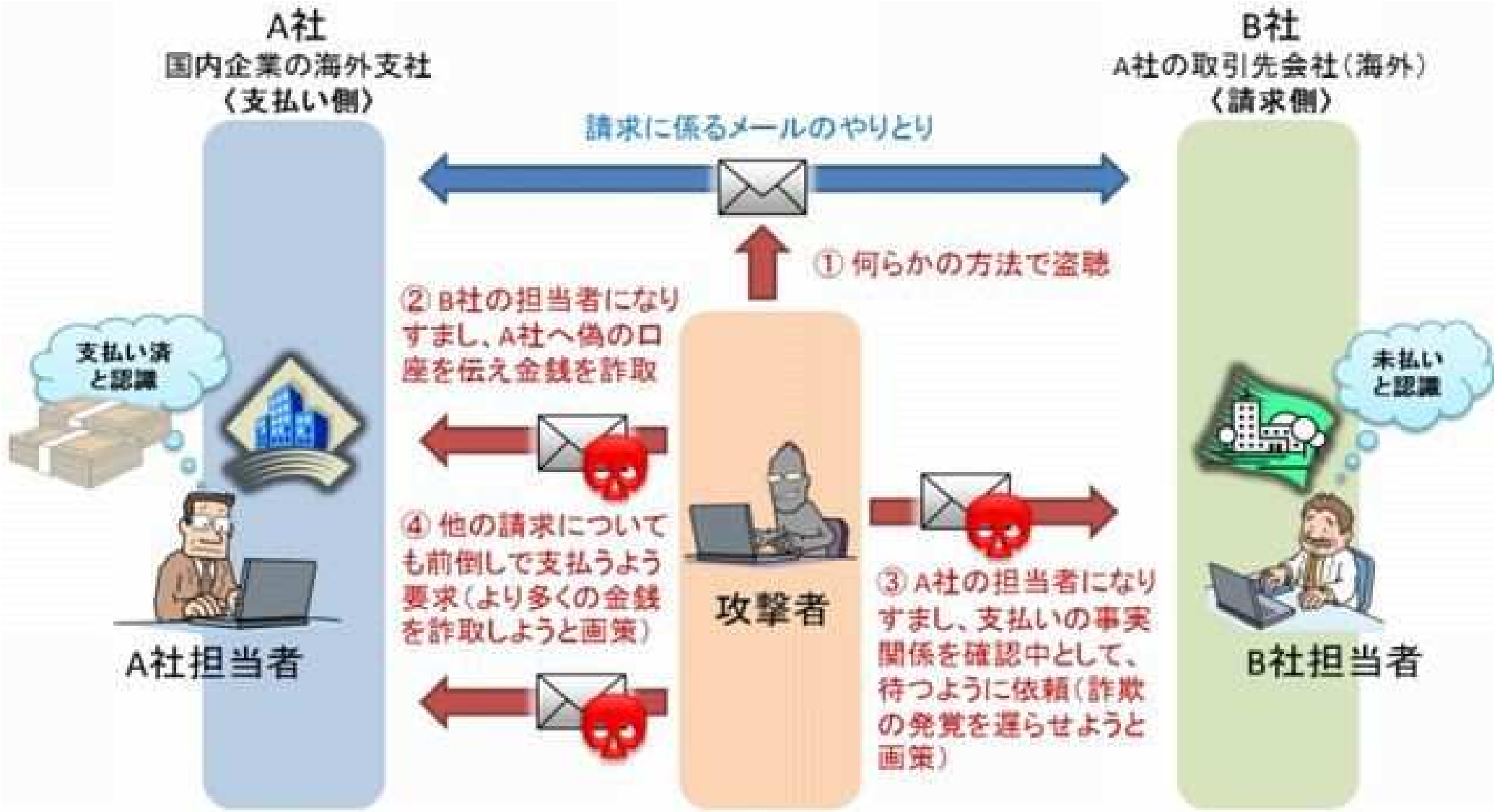
被害企業からは貴社が「加害者」に見える！

ビジネスメール詐欺の概要

BEC（Business Email Compromise）

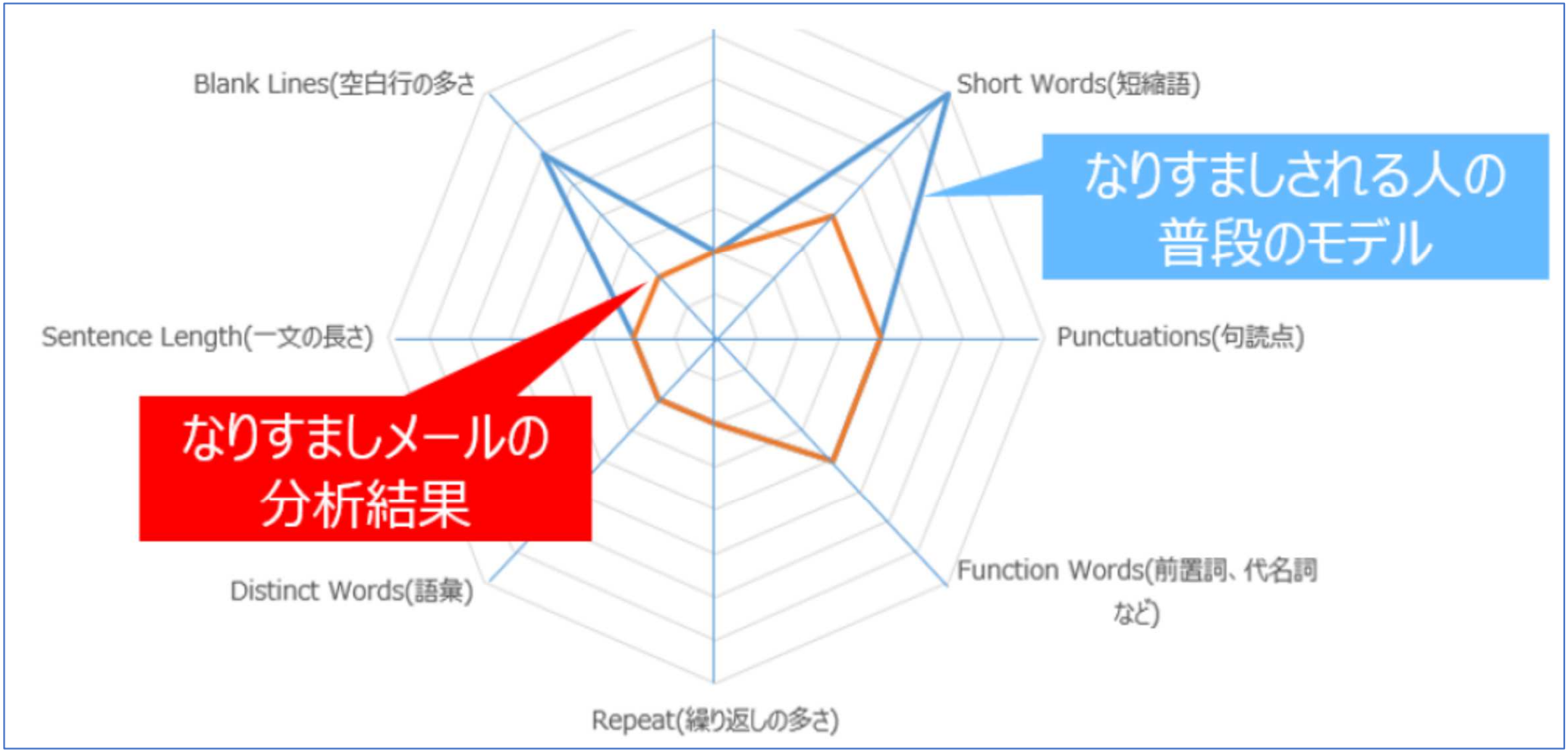
https://www.youtube.com/watch?v=sxybmE1rrZg （トレンドマイクロ）

https://www.youtube.com/watch?v=GZLZrnJQcts （カラーサイン機能）



ビジネスメール詐欺対策の新技術「Writing Style DNA」

- AI技術によってメール作成者の分の書き方の癖を分析し、なりすましメールを防ぐ仕組み。



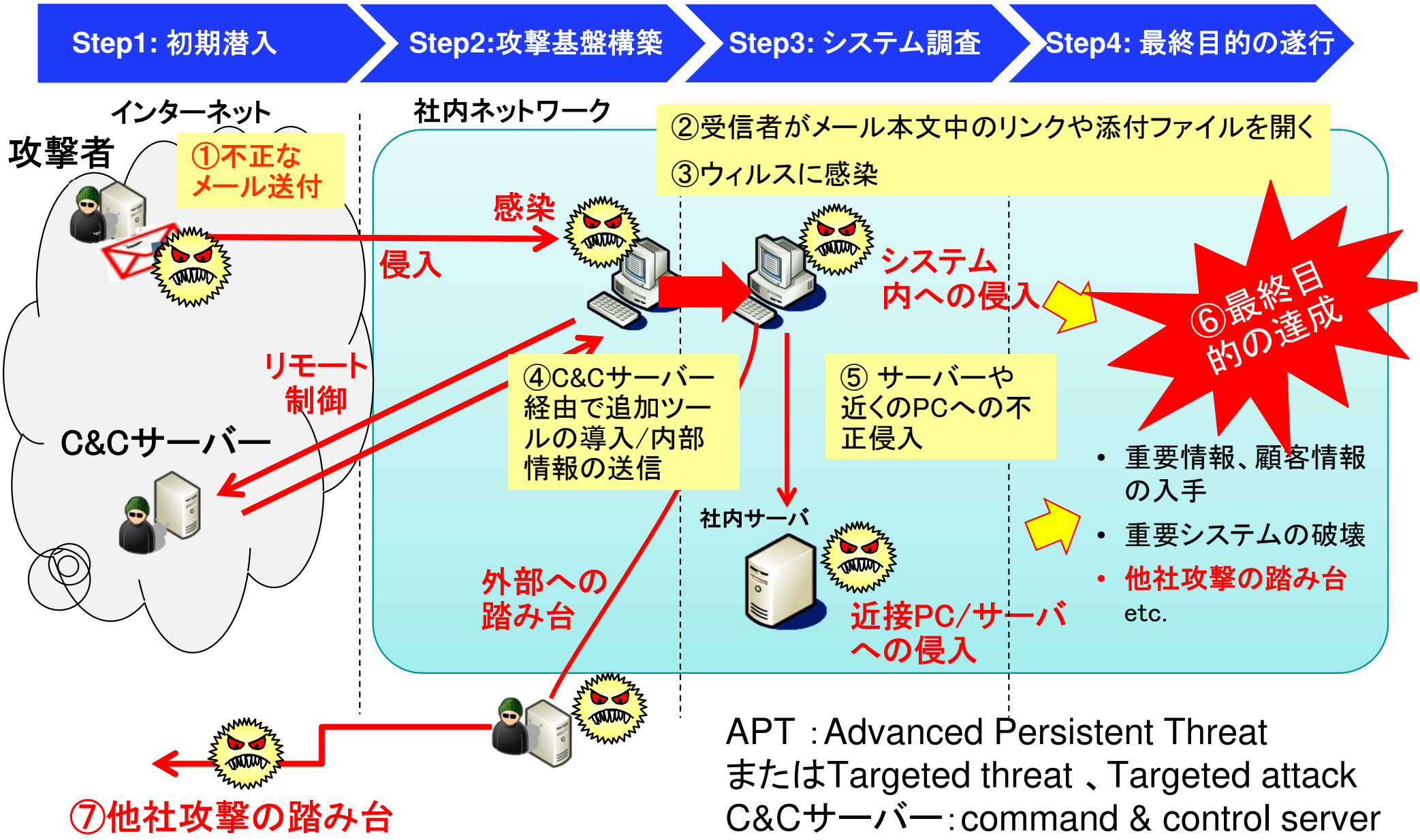
https://www.trendmicro.com/ja_jp/about/trendpark/Writing-Style-DNA-201903-01-01.html?mkt_tok=eyJpIjoiWldRMk1qWm1OREV6TjJZMiIsInQiOiIrN0J3amdZN1o1Rk83UmZkdmRRcmpoeE1DN2RLY1dmN

法人組織が知っておくべきビジネスメール詐欺の手口と対策

トレンドマイクロ株式会社

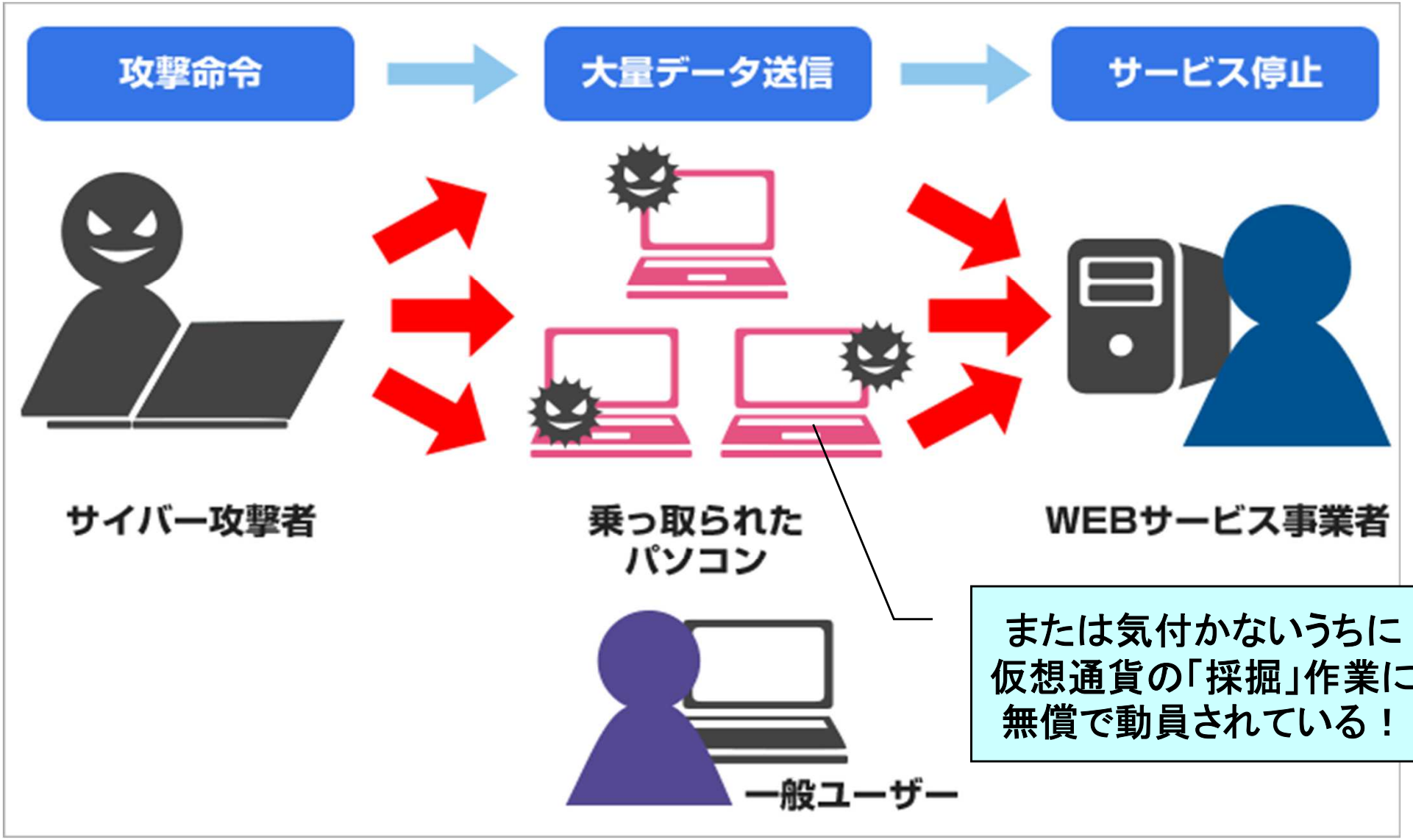
https://resources.trendmicro.com/jp-docdownload-form-m090-web-bec-whitepaper.html

標的型（APT）攻撃のパターン



APT ：Advanced Persistent Threat
またはTargeted threat 、Targeted attack
C&Cサーバー：command & control server

他社攻撃の踏み台（DDoS攻撃の手口）



DDoS（ディードス）攻撃・・・分散型サービス妨害攻撃（Distributed Denial of Service attack）

http://www.office-copy.com/knowledge/network/network8.html

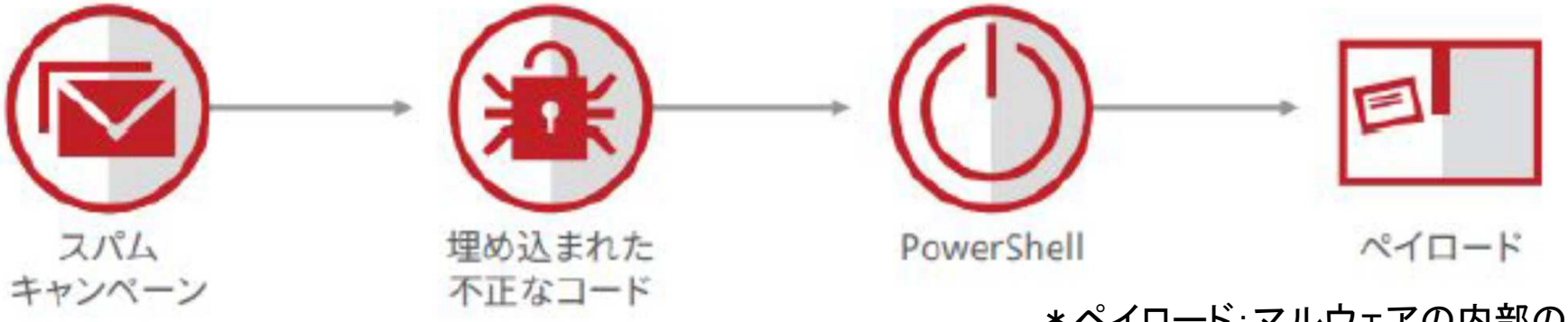
ファイルレスマルウェアの脅威

実行ファイルがないためディスク上に保存されず、メモリ上で実行されるマルウェア

- 従来のマルウェアは、メールの添付ファイル（.exe形式の実行ファイル）を開いたり、悪意のあるWebサイトにアクセスすることで感染する。ディスクに保存され、それが実行されることによって不正な動作を行う。
- ファイルレスマルウェアは実行ファイルがないため、「パターンファイル」（「定義ファイル」もしくは「シグネチャ」）のマッチング方式の従来型セキュリティ対策ソフトでは検知が困難（ステルス性が高い）。
- 「Windows PowerShell」や「Windows Management Instrumentation」を悪用し、スパムメールに埋め込んだコードからPowerShellなどに対して不正な指示を出す。

ファイルレスマルウェアの脅威 ！仕組みと感染経路からみる実践的対策
マカフィー公式ブログ　2019年5月29日

ファイルレス・マルウェアの感染経路



＊ペイロード：マルウェアの内部の悪意のある動作をするコードの部分のこと

PowerShellを悪用する感染例

1. メールに添付されたlnkの拡張子を持つファイルをクリック
2. PowerShellコードが実行され、このコマンドが外部サーバから不正なプログラムをダウンロードし、実行
3. この不正コードはディスク内にファイルを残さず、PC内のメモリに書き込みをし、lnkファイルは削除される
4. こうして攻撃者に乗っ取られたPowerShellは、外部のC&Cサーバーから不正に操作され、情報搾取や不正操作をされる

ファイルレスマルウェアの脅威 !仕組みと感染経路からみる実践的対策
マカフィー公式ブログ　2019年5月29日

ファイルレス・マルウェア対策

- シグネチャベース（「パターンファイル」や「定義ファイル」）のウイルス対策ソフトではなくEDR（Endpoint Detection and Response）製品など「総合セキュリティ対策ソフト」を使う
  - ✓EDR製品はエンドポイントで脅威の「検知」を行い「対応」をサポートする製品で、監視・情報収集、機械学習・動作分析により、エンドポイントに侵入してきた未知のマルウェアの検知・対応策として有効
  - ✓PowerShellの接続と同時にWordが起動したとしたら疑わしいため、そのプロセスを隔離・停止するなど怪しい行動を阻止するような措置を実施する。

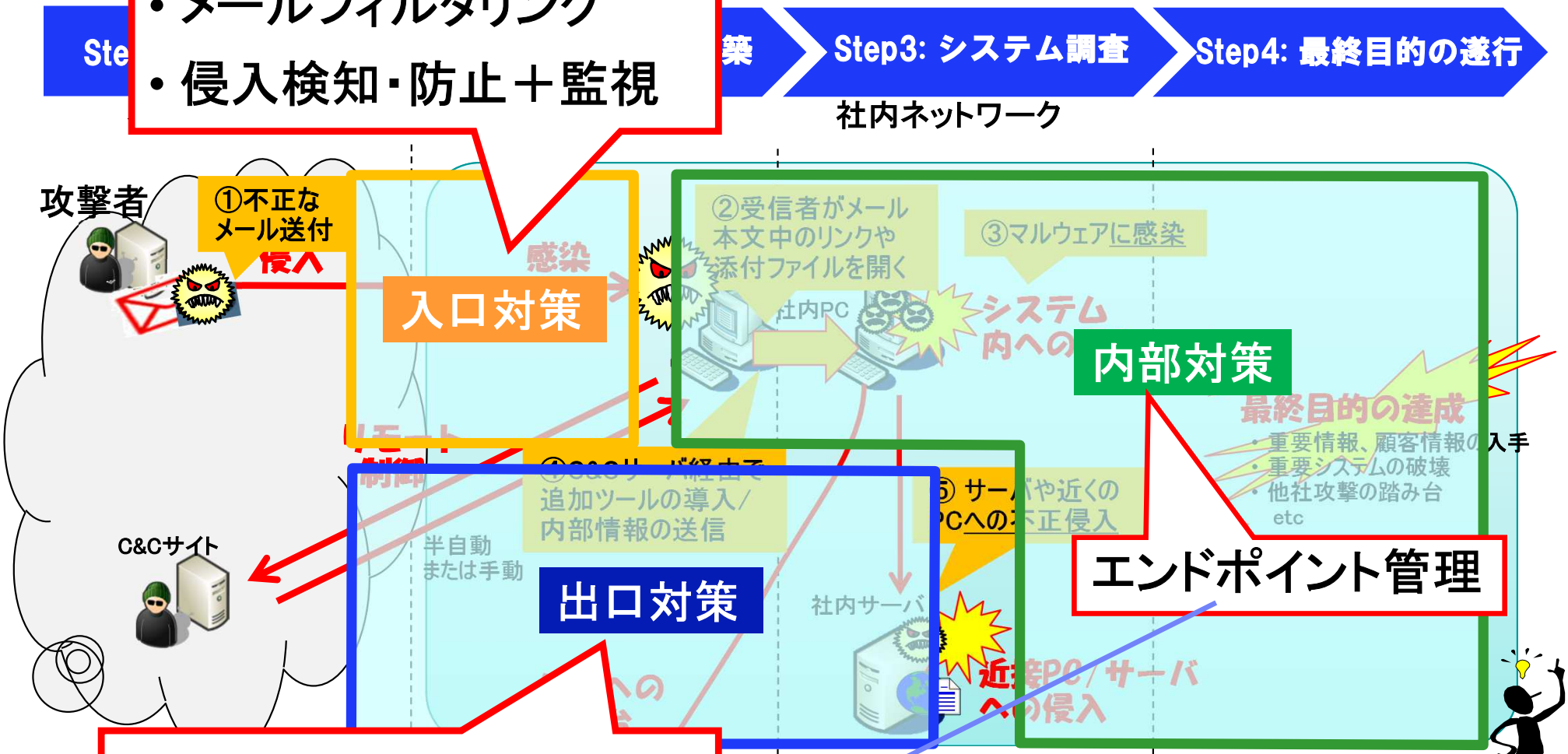
Endpoint（エンドポイント）
通信回線やネットワークの末端に接続された端末やコンピュータ、情報機器などのこと。

ファイルレスマルウェアの脅威 !仕組みと感染経路からみる実践的対策
マカフィー公式ブログ　2019年5月29日

三つの観点からのセキュリティ対策が必要！

- ファイアウォール
- メールフィルタリング
- 侵入検知・防止＋監視

EPP（Endpoint Protection Platform）：水際の防止策



- 侵入検知・防止＋監視
- 機密情報漏えい防止

EDR（Endpoint Detection and Response）：水際で防げない攻撃の「可視化」と「対応支援」

もくじ

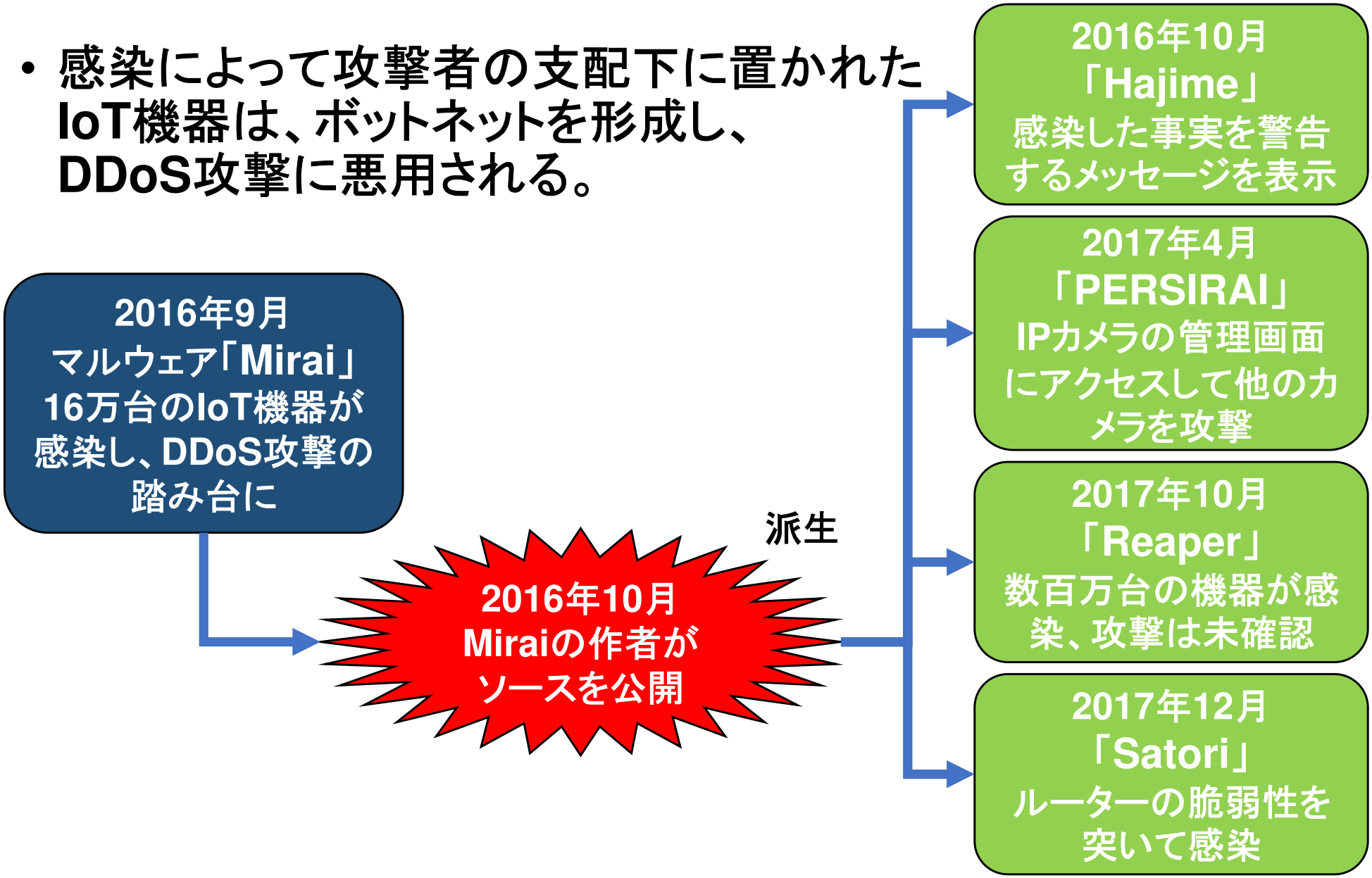
1. 情報システムセキュリティの現状と課題

2. IoT機器関連のセキュリティ脅威と課題

3. IoT関連セキュリティのトピックスと対策

マルウェア「Mirai」の脅威

- 感染によって攻撃者の支配下に置かれたIoT機器は、ボットネットを形成し、DDoS攻撃に悪用される。



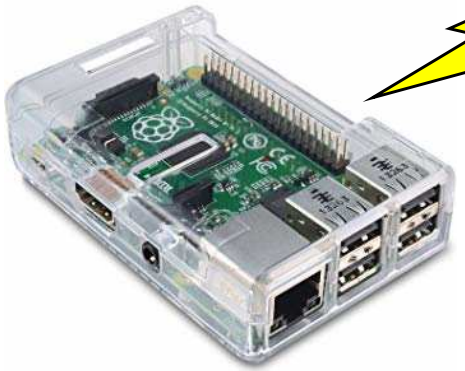
「IoTが危ない　5分に一度狙われる」 日経コンピュータ2018年5月10日号

「5分に一度狙われる」とは？

543分間に107件
→約5分に1回　IoT機器を
ターゲットとするアクセス

検証用マシン

ラズベリーパイを
グローバルIPを持
つSIMカードでイン
ターネット接続



543分間に
354個のIPアドレスから
798件のアクセス

内訳

23番ポート（Telnet）：86件
22番ポート（SSH）：21件

＊最多は445番ポート（Windowsファイル共有）の110件

「IoTが危ない　5分に一度狙われる」 日経コンピュータ2018年5月10日号

辞書攻撃

- IDやパスワードによく使われる文字列を使って不正ログインを行う攻撃。Webサービスに不正ログインする攻撃手法の定石。

IoTウイルスの辞書攻撃に使う認証情報(ID/パスワード)の例

666666/666666	admin/meinsm	root/1111	root/dreambox	root/user
888888/888888	admin/pass	root/1234	root/hi3518	root/vizxv
admin/(なし)	admin/password	root/12345	root/ikwb	root/xc3511
admin/1111	admin/smcadmin	root/123456	root/juantech	roo/xmhdipc
admin/1111111	admin1/password	root/54321	root/jvbzd	root/zlxx.
admin/1234	administrator/1234	root/666666	root/klv123	root/Zte521
admin/12345	Administrator/admin	root/7ujMko0admin	root/klv1234	service/service
admin/123456	guest/12345	root/7ujMko0vizxv	root/pass	supervisor/supervisor
admin/54321	guest/guest	root/888888	root/password	support/support
admin/7ujMko0admin	mother/fucker	root/admin	root/realtek	tech/tech
admin/admin	root/(なし)	root/anko	root/root	ubnt/ubnt
admin/admin1234	root/00000000	root/default	root/system	user/user

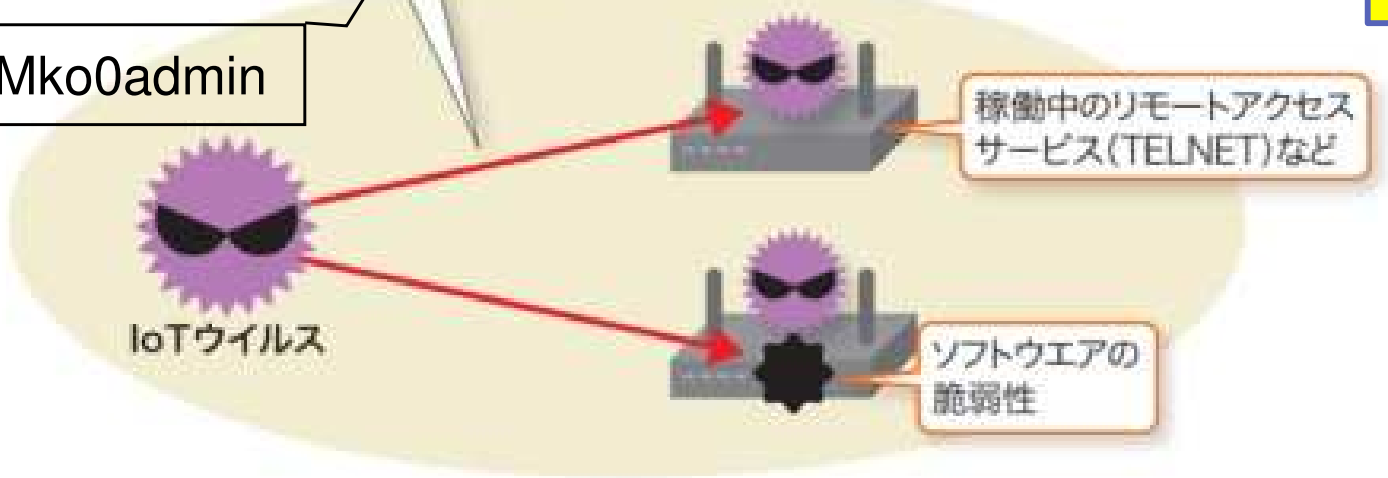
初期のMiraiが使っていた60通りの辞書

メーカーの工場出荷時の初期値など

現在は亜種ウィルス開発の活発化で組合せが数千に上るとも・・・

これのどこが問題？

7ujMko0admin



日経 xTECH　2019/05/28　**ミライ・ハジメ・サトリ…、IoTウイルスはなぜ増えるのか**
https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00763/052000002/

IoTセキュリティ被害事例①

自動車へのハッキング

- Jeep Cherokeeの車載機Uconnectに認証回避の脆弱性があり、悪意あるファームウェアに書換え可能
- UconnectにはIPアドレスが割り振られており、遠隔から操作可能
- ファームウェアを改ざんした車に対して攻撃コードを送りこむことで、ブレーキ、ステアリング、エアコン等への干渉が可能
- 米FCAUS（旧クライスラー）は140万台をリコール、修正ソフトはオーナ及び整備工場にUSBメモリで配布

https://www.youtube.com/watch?v=MK0SrxBC1xs

たった2500円の自動車ハッキングツール

セキュリティ対策への
の警鐘となるか？
愉快犯を増殖させる
ことにならないか？

ハッキングされた
自動車が起こした
事故は誰の責任？

ブラックハットUSAにセキュリティ企業「360」が出展
http://geekcar.com/archives/68050

IoTセキュリティ被害事例②

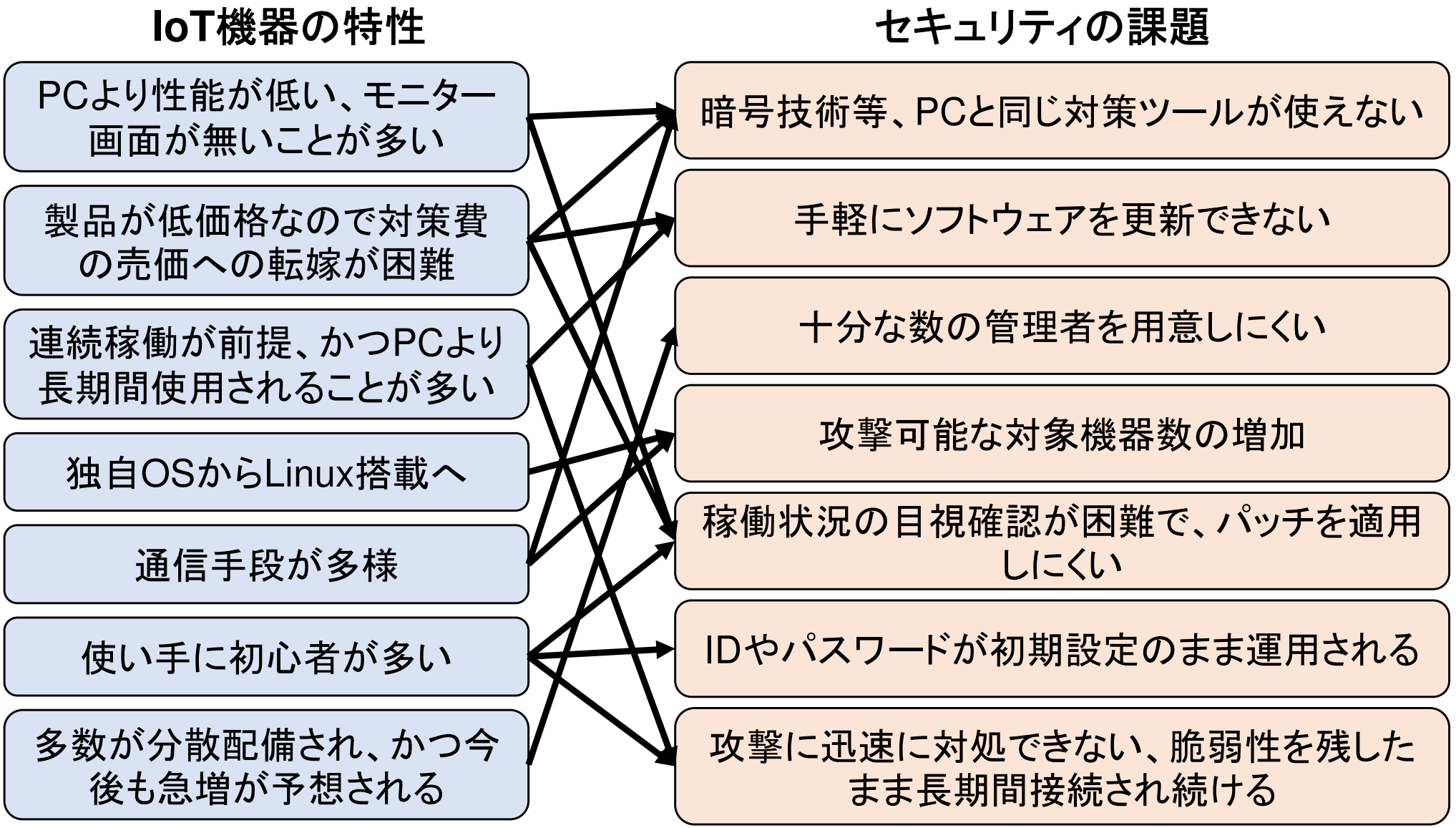
Webカメラの画像を意図しない相手が見ることが可能

- IPアドレス等から2,163台のWebカメラを検出、内769台でパスワードが未設定
（設定されていてもデフォルトパスワードのケースも）
- 非公開の試作品や店舗や工場の様子が確認できた
- 場所を特定できたケースや、カメラの向き等を第三者が操作できた可能性も
- ハッキングされたWebカメラから画像がYouTubeへ・・・？

https://blog.kaspersky.co.jp/2ch-webcam-hack/11220/

独立行政法人情報処理推進機構 「IoTにおけるセキュリティの脅威と対策」

IoT機器の特性から見たセキュリティの課題



「IoTが危ない　5分に一度狙われる」 日経コンピュータ2018年5月10日号を基に作成

もくじ

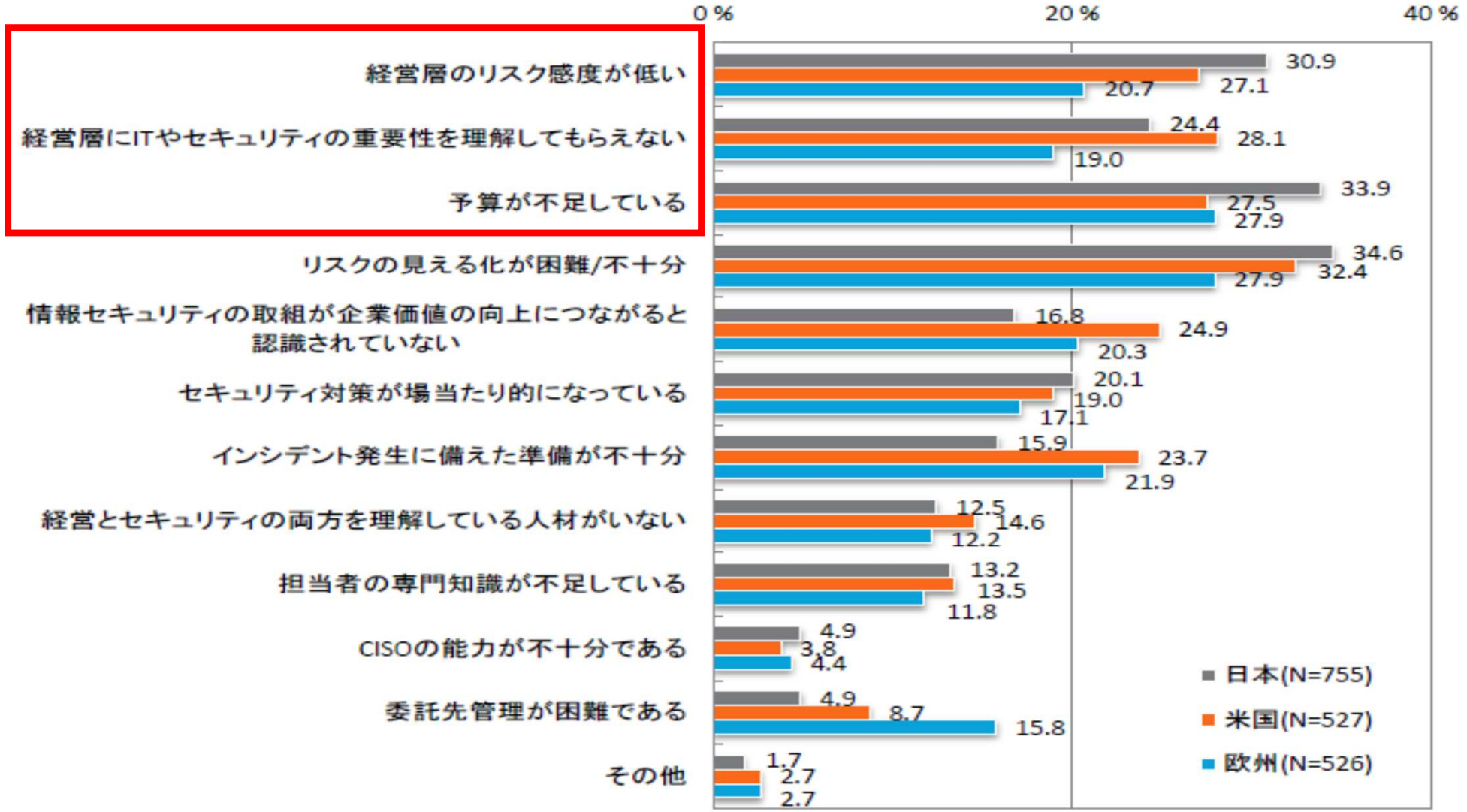
1. 情報システムセキュリティの現状と課題

2. IoT機器関連のセキュリティ脅威と課題

3. IoT関連セキュリティのトピックスと対策

情報セキュリティ対策推進上の課題

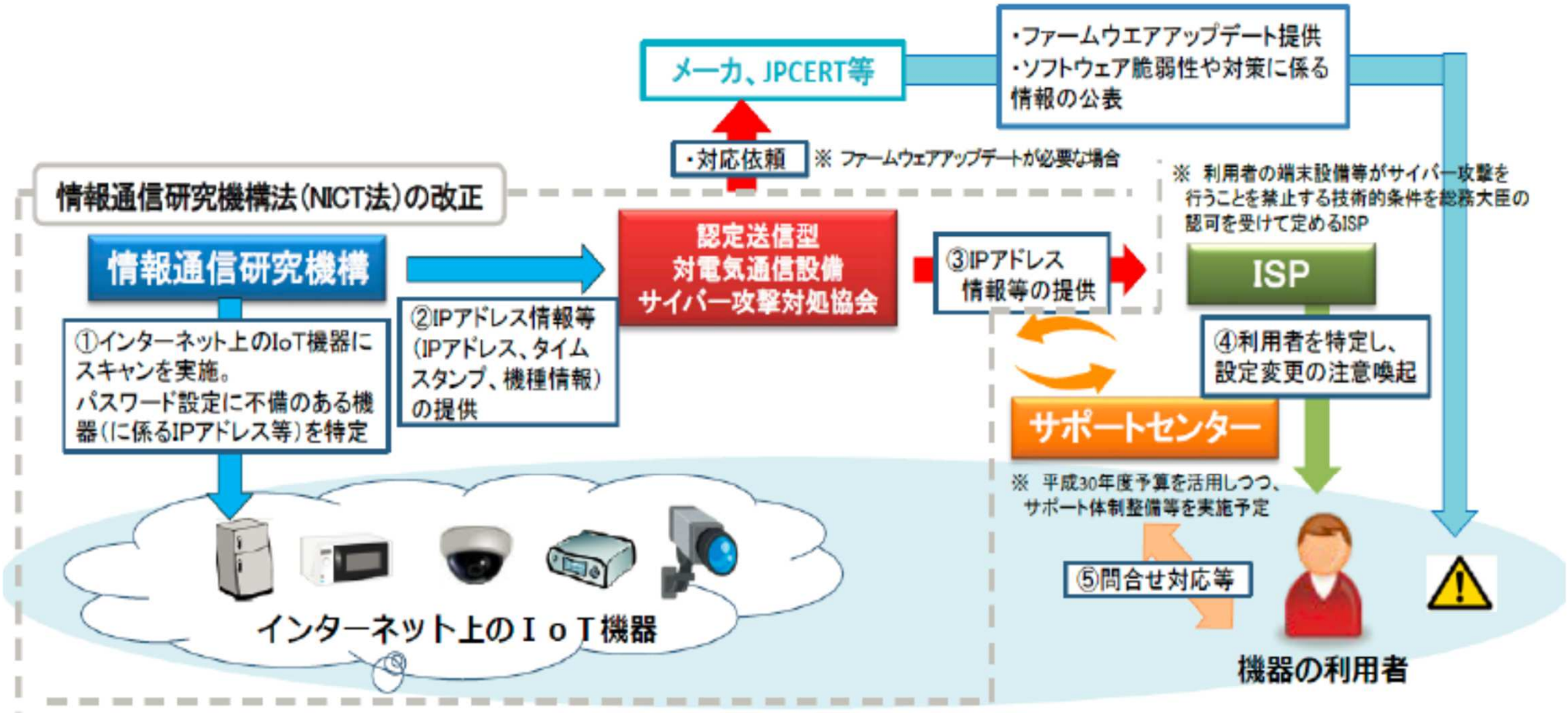
- 経営層の認識に起因する課題が多く挙げられています。



独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017-調査報告書-」

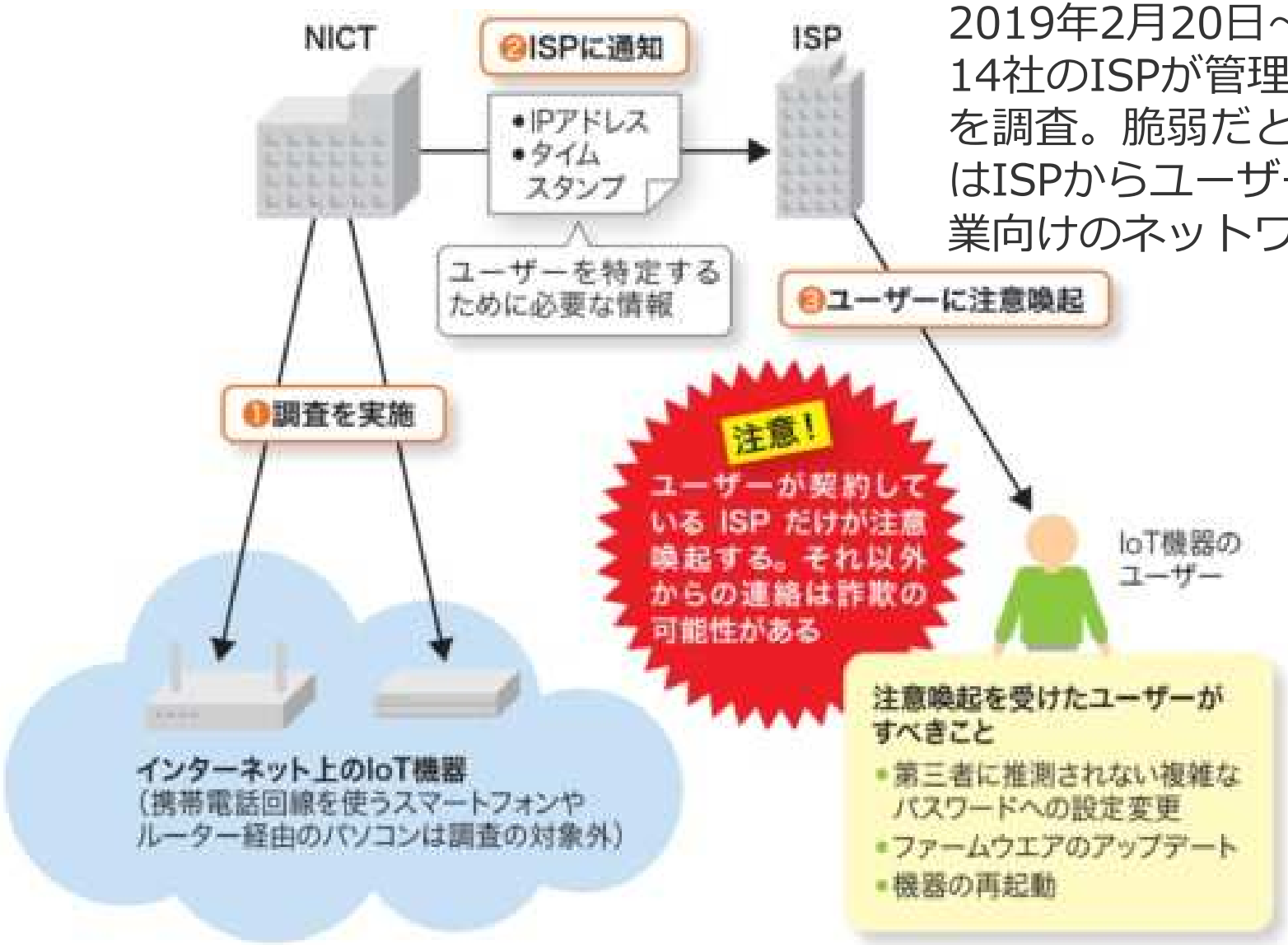
情報通信研究機構によるIoT機器調査

- 総務省所管の情報通信研究機構（NICT）が、攻撃の標的になりやすい脆弱な機器を調査できるように、NICT法を改正（2023年までの時限措置）



総務省サイバーセキュリティ統括官付参事官　木村公彦
「総務省におけるIoTセキュリティの取組について」

国家プロジェクト「NOTICE」



2019年2月20日～4月の間
14社のISPが管理する4000万アドレスを調査。脆弱だと判断されたIoT機器はISPからユーザーに注意喚起。（企業向けのネットワーク製品が中心）

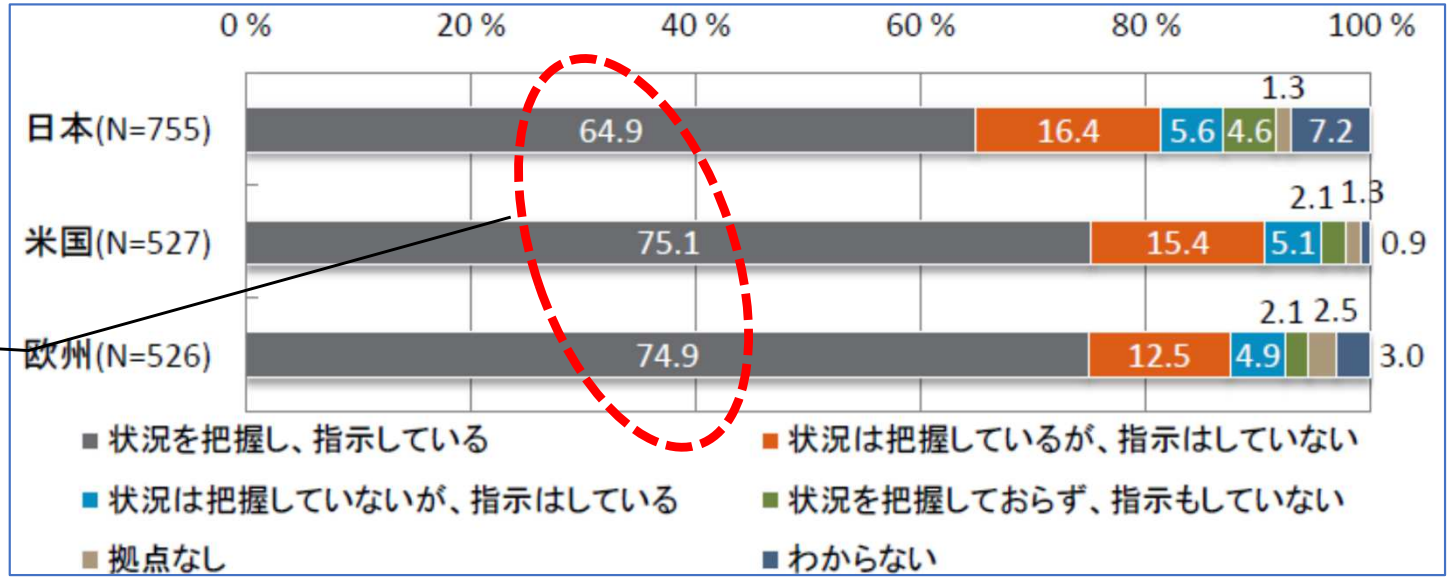
NICT（国立研究開発法人情報通信研究機構
：総務省所管）
National Institute of Information and Communications

ISP： Internet Service Provider

日経 xTECH　2019/05/29　**国家施策「NOTICE」から最初に注意されたあの製品**
https://tech.nikkeibp.co.jp/atcl/nxt/column/18/00763/052000003/

取引先のサイバーセキュリティ対策把握の遅れ

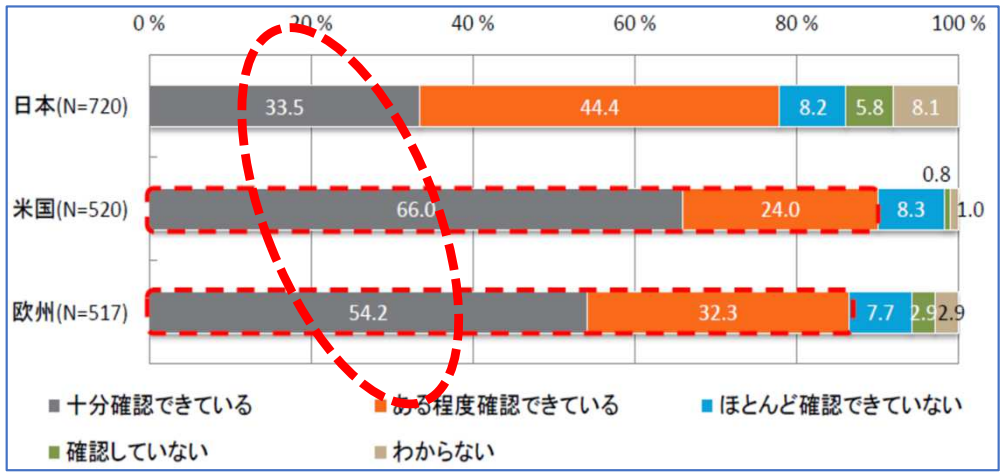
自社拠点のセキュリティ
対策把握状況（国内拠点）



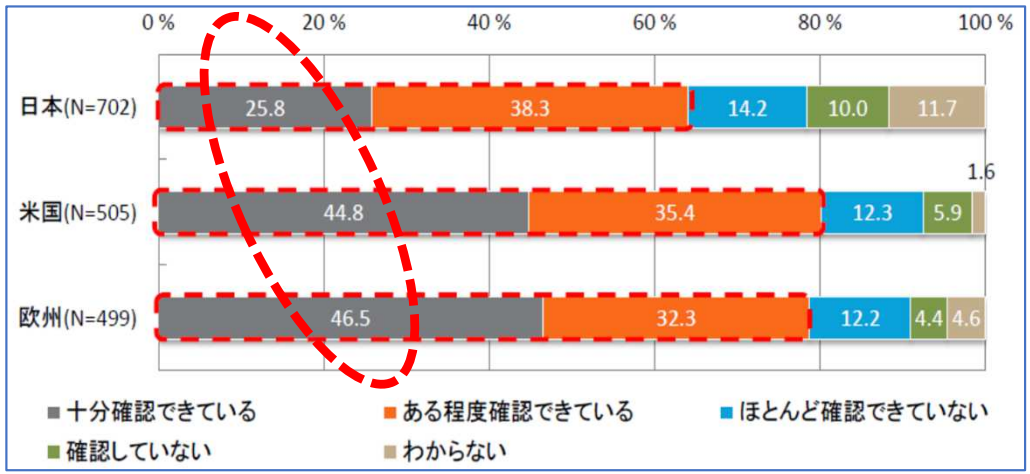
欧米よりやや低い程度

いずれも大幅に低い！

「**業務委託先**」のセキュリティ対策把握状況



「**物品調達先**」のセキュリティ対策把握状況



独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017-調査報告書-」

IoT機器のセキュリティ対策（短期版）

「当たり前」のことを確実に。（凡事徹底）

1.IoT機器の再起動
- 揮発型のマルウェアを消滅させる。

2.ID/パスワードの管理
- 初期パスワードを定期的に変更し、侵入を防ぐ。取り扱い説明書を読み、正しい設定や使い方を理解・確認する。

3.ファームウェアのアップデート
- バージョンアップやパッチ適用の徹底。しかし売り切り型の機器では困難。

4.インターネット側からのアクセス拒否設定
- 外から繋がせない。

5.ゲートウェイ機器の内側に設置
- 直接インターネットに繋がない。

6.古い機器は買い換える
- 自動アップデート機能がない機器はNG。

7.セキュリティ教育や操作指導の徹底
・最新の攻撃手口や被害例を周知徹底する。

第3回IoTセキュリティフォーラム　パネル・ディスカッションを基に作成

IoTセキュリティ設計の手順

Phase1:脅威分析	Step 1	対象とするIoT製品やサービスのシステム全体構成を明確化する。
	Step 2	システムにおいて、保護すべき情報・機能・資産を明確化する。
	Step 3	保護すべき情報・機能・資産に対して、想定される脅威を明確化する。
Phase2:対策検討	Step 4	脅威に対抗する対策の候補（ベストプラクティス）を明確化する。
	Step 5	どの対策を実装するか、脅威レベルや被害レベル、コスト等を考慮して選定する。

必要不可欠な脆弱性への対応
（IoT機器提供者向け）

	脆弱性への対応内容
開発段階での対応	(1) 新たに脆弱性を作り込まないこと
	(2) 既知の脆弱性を解消すること
	(3) 残留している脆弱性を検出・解消すること
	(4) 製品出荷後の脆弱性の新たな発見に備えること。
運用段階での対応	(1) 継続的な脆弱性対策情報の収集
	(2) 脆弱性対策情報（更新ソフトウェアを含む）の作成
	(3) 脆弱性対策情報の利用者への通知
	(4) 更新ソフトウェアの製品への適用

情報処理推進機構 「IoT開発における セキュリティ設計の手引き」

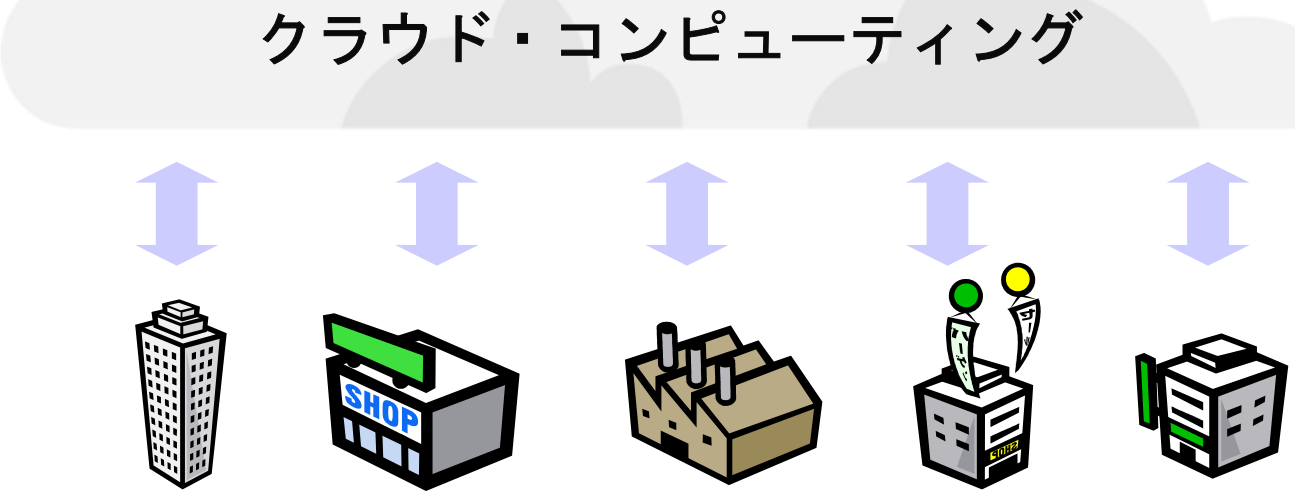
中小企業の情報セキュリティ対策ガイドライン

IPA
独立行政法人 情報処理推進機構
技術本部 セキュリティセンター

クラウド･コンピューティングの価値

- 柔軟性の高い処理能力
- 従量制課金
- システム導入や構築期間の短縮

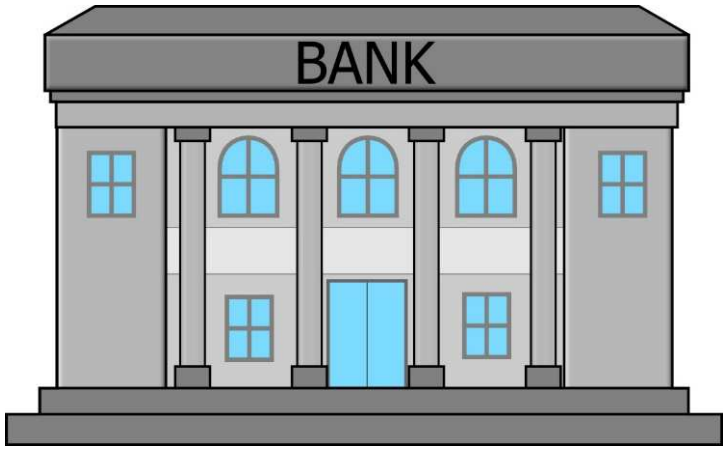
ポイント
自社でサーバーを持たない



銀行預金とタンス預金

どちらが
安全？

銀行預金
セキュリティー対策が施されたITベンダーのクラウド・コンピューティング



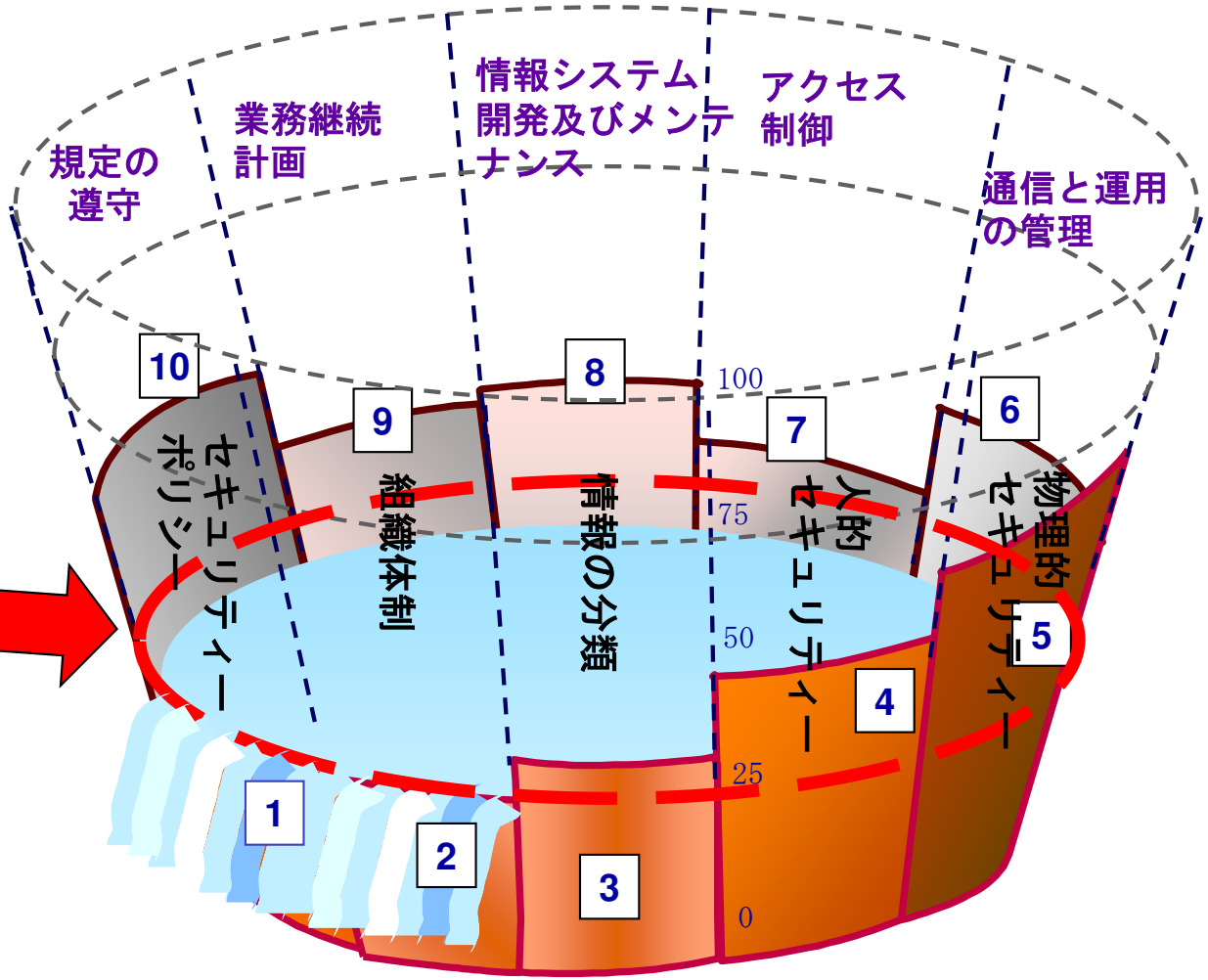
タンス預金
自社サーバー（オンプレミス）によるシステム運用

情報セキュリティー監査

企業のセキュリティーでは最低の箇所が全体のレベルとなる！

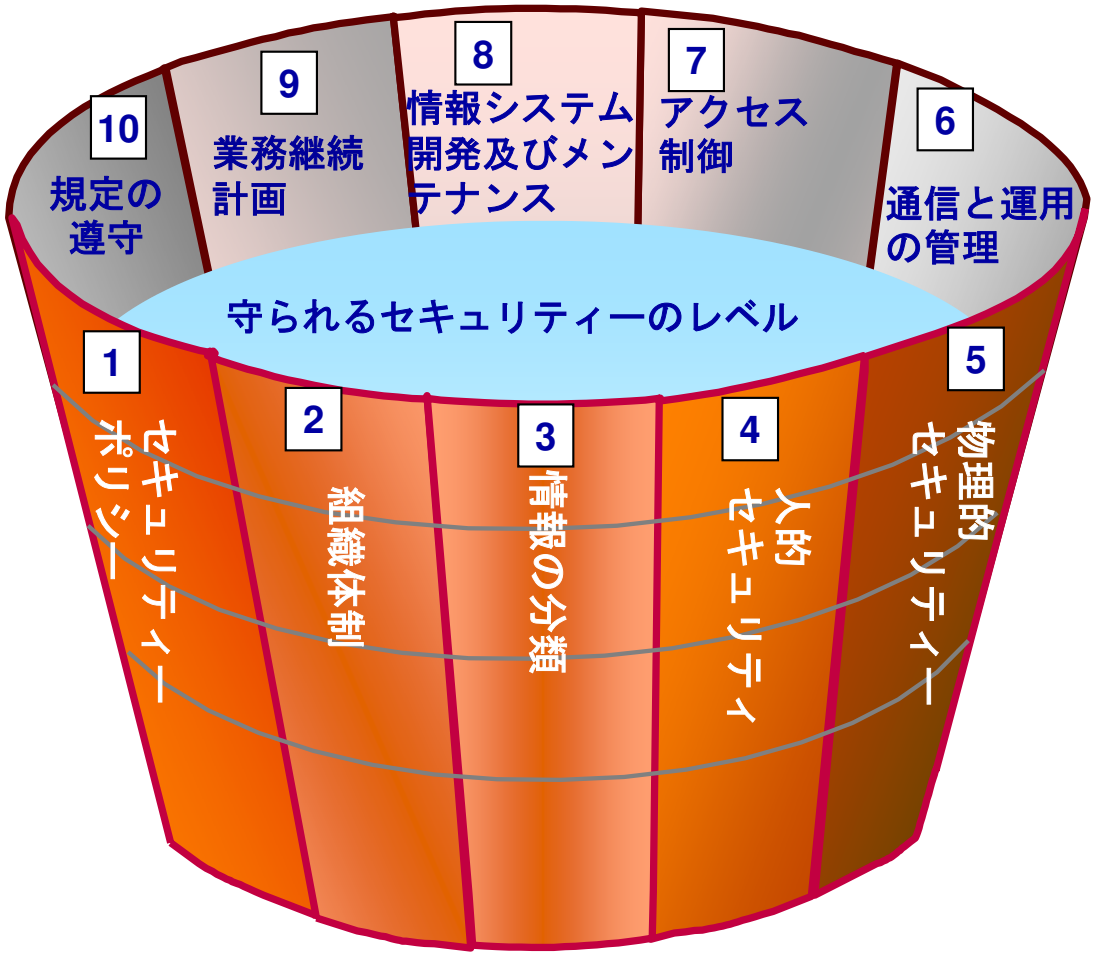
従業員から「うっかり八兵衛」を出さないようにするためには？

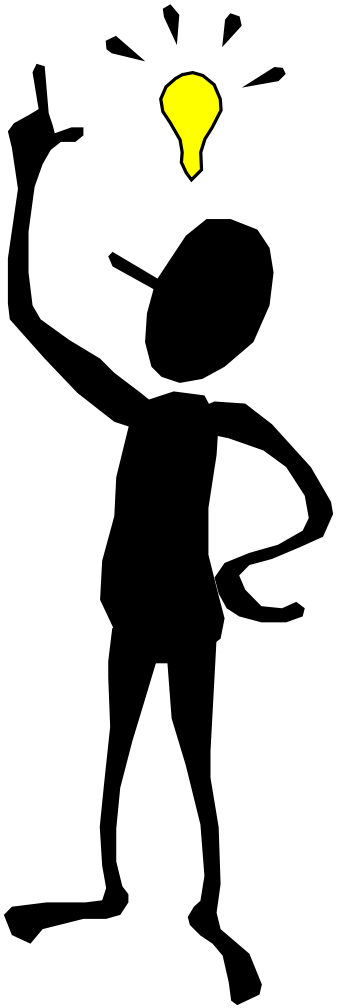
最低ライン



目指す姿

こうなっていればOK！





情報セキュリティーの桶

本教材利用上の注意事項