\Orchestrating a brighter world NEC

ITmedia Security Week 2022夏
”高度セキュリティ人材”と”アウェアネス“

セキュリティ人材の両輪でビジネスに勝つ

2022年6月13日
NECサイバーセキュリティ戦略統括部
統括部長　淵上 真一,CISSP

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

自己紹介

淵上 真一

サイバーセキュリティ戦略統括部 統括部長

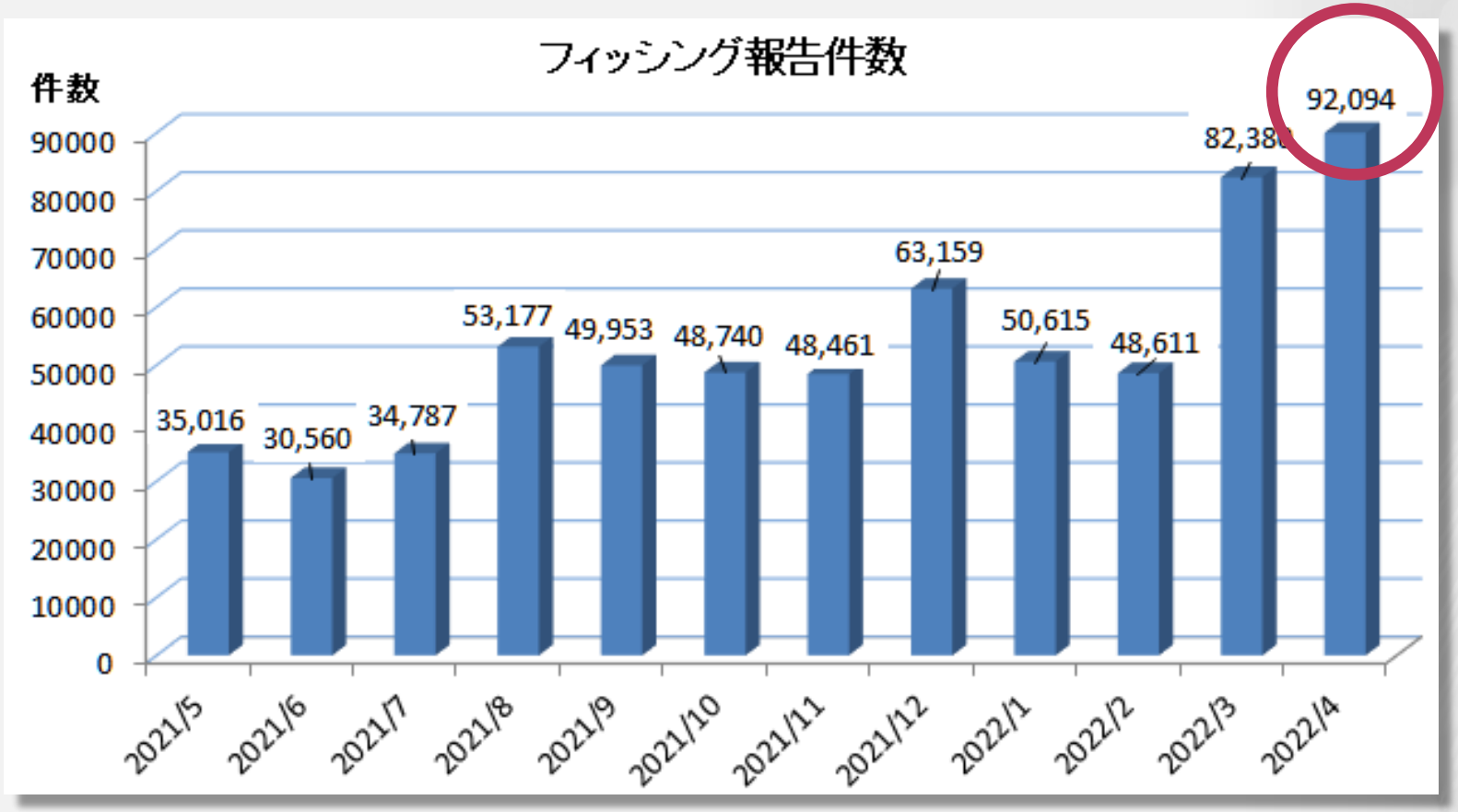
ベンチャー系システムインテグレータで
ネットワークエンジニアを経て、
専門学校グループを運営する学校法人に転職

組織のセキュリティコントロールを担当する傍ら、
司法、防衛関連のセキュリティトレーニングを手掛ける

2018年よりNEC

- (ISC)² 認定主任講師
- Cisco Networking Academy Instructor Trainer
- 情報処理安全確保支援士 集合講習認定講師
- 沖縄オープンラボラトリ
  Professional育成プログラム アドバイザー
- Hardening Project 実行委員

急増するフィッシング詐欺



2021/5月～2022/4月のフィッシング報告数(フィッシング対策協議会)
出典: https://www.antiphishing.jp/report/monthly/202204.html

4月の国内の
フィッシングの
報告数は
過去最多

再拡大を広げる「Emotet」

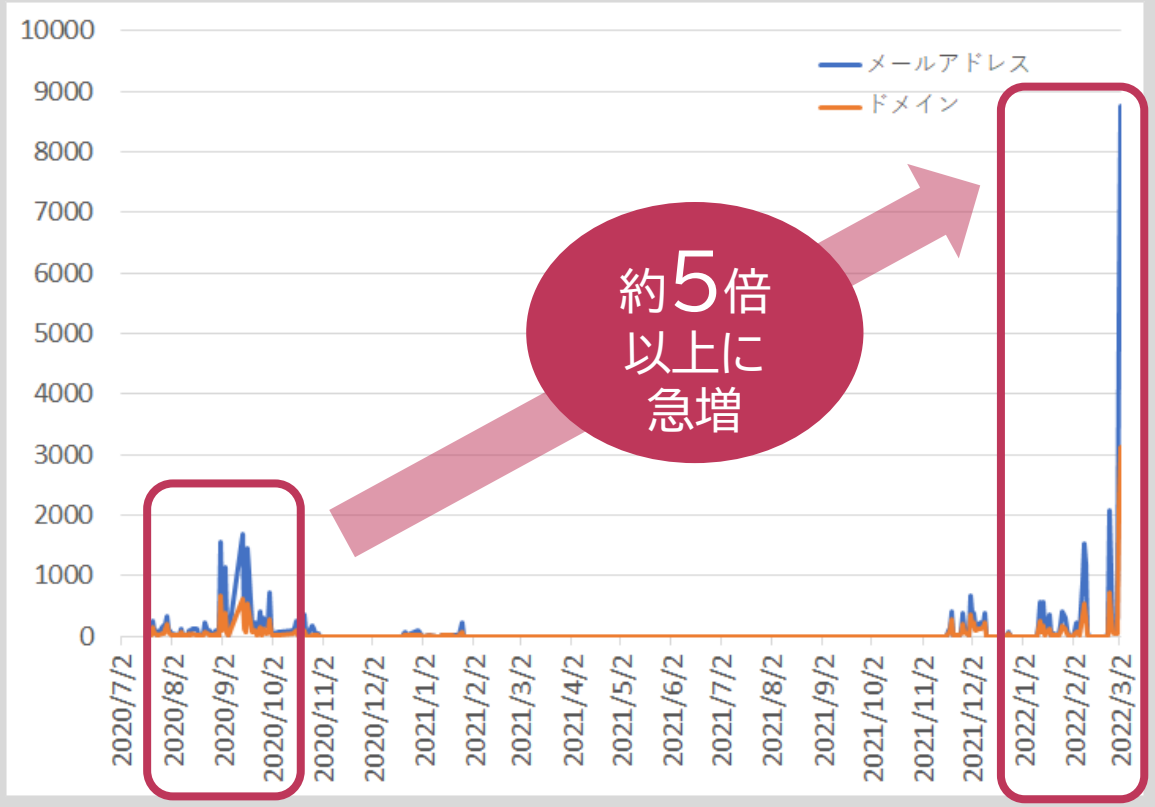
マルウェア「Emotet」の感染が再拡大、2022年2月の第一週より急速に拡大

マルウェア「Emotet」の感染再拡大に関する注意喚起（JPCERT/CC、2022/3/14 更新）

- 2022年3月に入り、「Emotet」に感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の約5倍以上に急増
- **国内感染組織から国内組織に対するメール配信も増加**

2021年1月に世界中の法執行機関によりテイクダウン作戦が行われていた（11月14日以降、活動再開が報告されていた）

Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移（JPCERT/CC）



引用：https://www.jpcert.or.jp/at/2022/at220006.html

攻撃者グループの分類

被害事例からみると**経済目的のサイバー犯罪者**が最も多くを占めている

被害報告からは、**経済目的のサイバー犯罪が大多数**を占める

2020 CRIME TYPES

By Victim Count

Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	241,342	Other	10,372
Non-Payment/Non-Delivery	108,869	Investment	8,788
Extortion	76,741	Lottery/Sweepstakes/Inheritance	8,501
Personal Data Breach	45,330	IPR/Copyright and Counterfeit	4,213
Identity Theft	43,330	Crimes Against Children	3,202
Spoofing	28,218	Corporate Data Breach	2,794
Misrepresentation	24,276	Ransomware	2,474
Confidence Fraud/Romance	23,751	Denial of Service/TDoS	2,018
Harassment/Threats of Violence	20,604	Malware/Scareware/Virus	1,423
BEC/EAC	19,369	Health Care Related	1,383
Credit Card Fraud	17,614	Civil Matter	968
Employment	16,879	Re-shipping	883
Tech Support	15,421	Charity	659
Real Estate/Rental	13,638	Gambling	391
Advanced Fee	13,020	Terrorism	65
Government Impersonation	12,827	Hacktivist	52
Overpayment	10,988		

国家背景の攻撃者

IC3の報告では明記されていない

報告数の大多数は経済目的の犯罪者

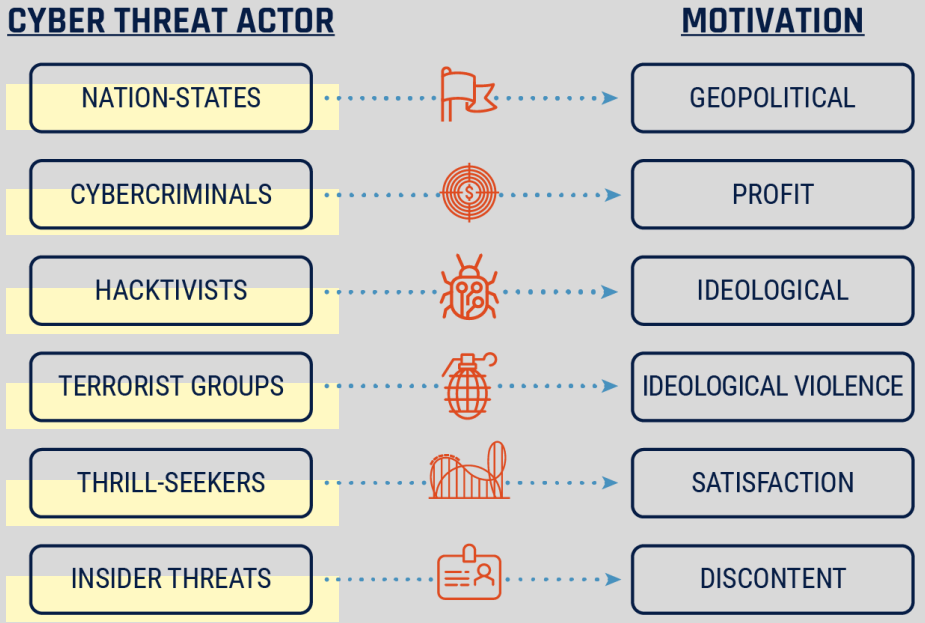
内部犯行は2%程度

テロリズム、ハクティビストの報告はごくわずか

米インターネット犯罪センター(IC3)への被害報告数

引用元:https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

アクター名で識別される**国家背景の攻撃者**も存在は無視できない



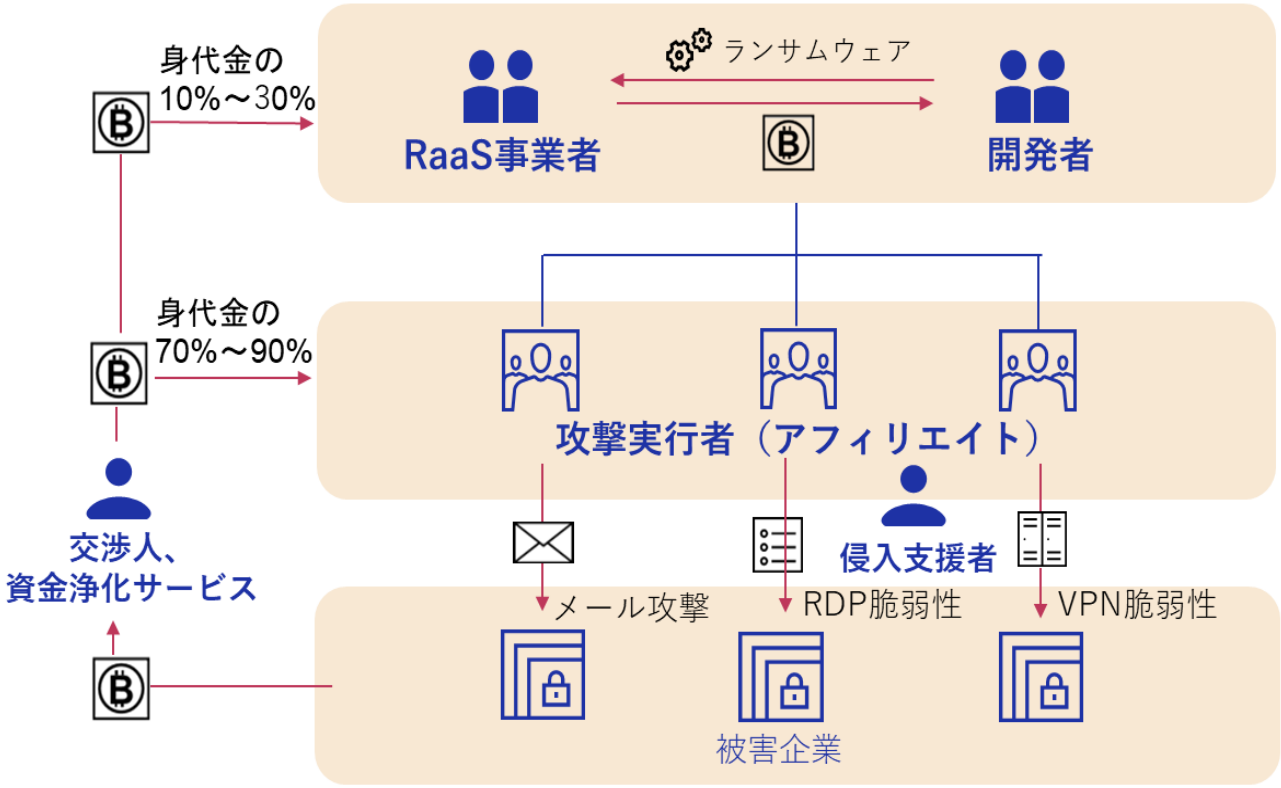
代表的な攻撃者の分類(例)

引用元:https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

経済目的の犯罪者のトレンド

2015年には経済目的の犯罪者は組織化されて活動しているとの報告
ランサムウェアをサービスとして扱うビジネスモデルが定着していると見られる

RaaS(Ransomware as a Service)のエコシステム



年商1億ドル以上の大手企業が標的
KELA社調査レポート

- 「道徳規範」や「支払い能力」を重視し、
  医療や教育機関、政府系組織を避けて、大手企業をターゲット
- 日本企業への攻撃も増大(不正メール検知:日本 第1位)

攻撃の分業化・ビジネス化が進み、闇市場も拡大

- 攻撃の各段階で専門家が対応する“JOB型”攻撃が確立
- 攻撃インフラ(RaaS)の利用により、簡単に攻撃可能
- 企業NWへの侵入に必要な情報は、闇市場で売買

サイバー攻撃総被害額年間660兆円
(日本のGDPを上回る金額)

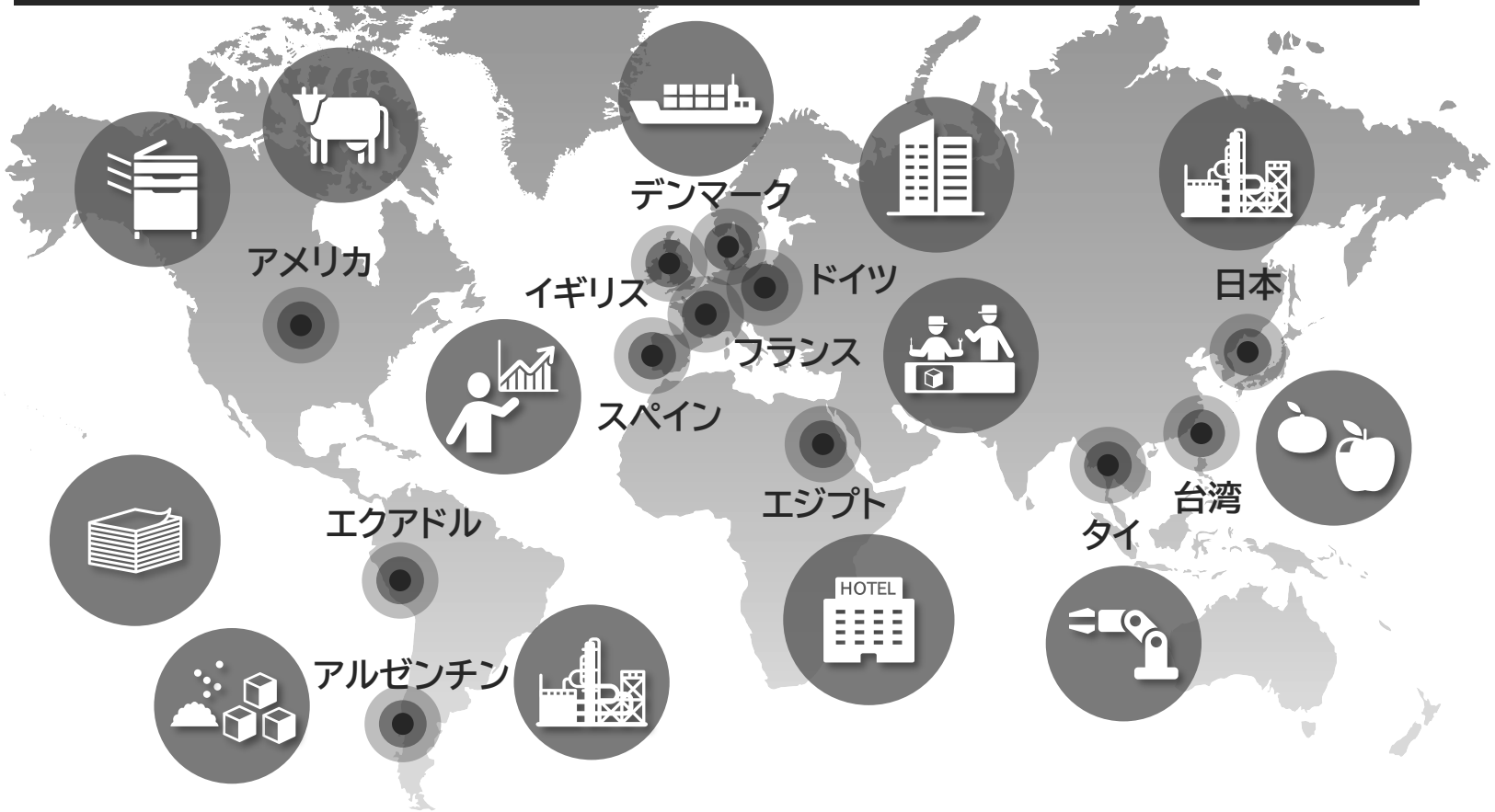
ランサムウェア被害額 2021年約200億ドル
(約2兆1000億円)

- 2015年の57倍、、2031年までに2650億ドル(28兆円)
- 2031年まで、2秒に1回ランサムウェア攻撃が発生

ランサムウェアの被害組織

様々な国、多種多様な業種にわたるランサムウェアの被害組織
特定の業種を狙うことで収益を上げていた様子も明らかになっている

LockBit 2.0のデータ漏洩被害組織（例）



ランサムウェアのリークサイト

DXを支えるトラストなサイバー空間のあり方

ゼロトラスト＋サイバーハイジーンがDXのセキュリティのベースに

ペリメタモデル

脅威は外側から
守るものは内側

クローズドな世界
（自分のところ）は
安全である

ゼロトラスト

脅威はあらゆる場所に

信頼の積み重ね

Security By Design

＋

サイバーハイジーン（公衆衛生）

全てのITの衛生管理を徹底
＜NISCや経団連も提唱(*)＞

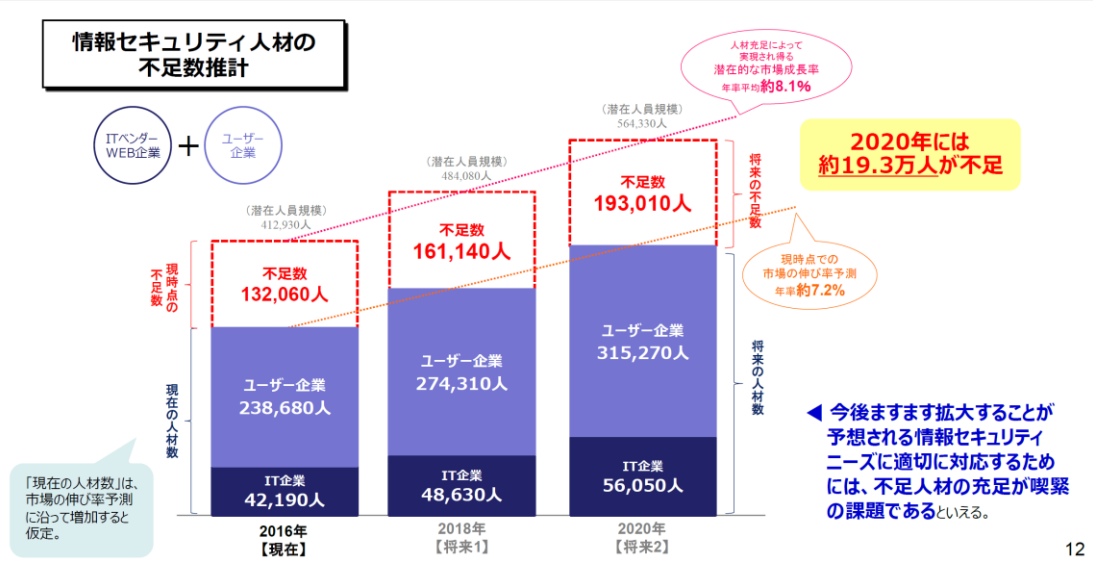
日常の運用で予防

Security Awareness

(*)サイバーセキュリティ意識・行動強化プログラム（内閣サイバーセキュリティセンター「NISC」）https://www.nisc.go.jp/active/kihon/pdf/awareness2019.pdf
Society5.0実現に向けたサイバーセキュリティの強化を求める（日本経済団体連合会） https://www.keidanren.or.jp/policy/2017/103_honbun.pdf

セキュリティ人材不足はどうなったのか

2020年には
19.3万人が不足するとして
様々な対策が実施された…



グラフ出典:IT人材の最新動向と将来推計に関する調査結果 ～ 報告書概要版 ～、
経済産業省 商務情報政策局 情報処理振興課、平成28年6月10日
https://www.meti.go.jp/shingikai/economy/daiyoji_sangyo_skill/pdf/001_s02_00.pdf

独立行政法人 情報処理推進機構 社会基盤センター「IT人材白書2020」によると

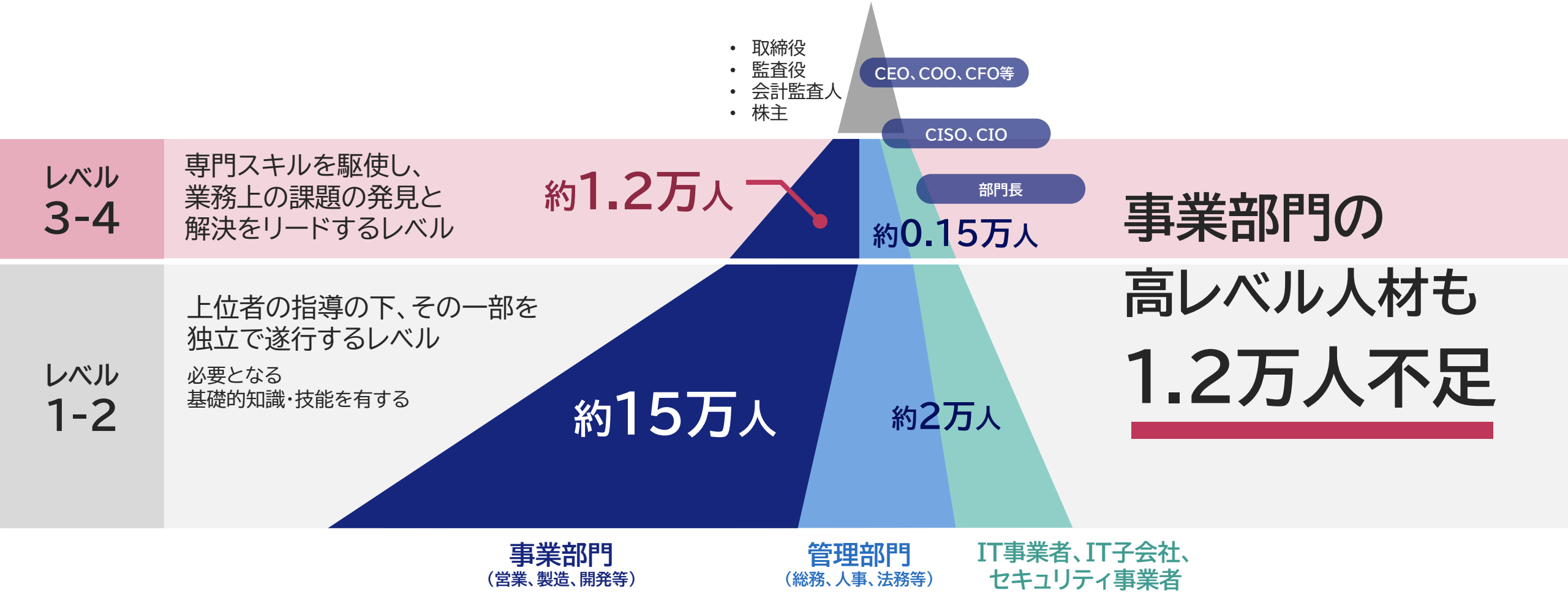
情報セキュリティ専門技術者を
「確保できている」と回答した
ユーザ企業は**6.2%**

政府機関も人材を募集

https://www.mod.go.jp/j/saiyou/internal/hijoukin/hijoukin_saiyou_202104.html

解消しないセキュリティ人材不足

セキュリティ人材不足数の各部門とスキルレベルとのマッピング



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/pdf/report/Human-Development-Plus-Security.pdf を元にNEC作成

DXを支えるトラストなサイバー空間のあり方

ゼロトラスト＋サイバーハイジーンがDXのセキュリティのベースに

ペリメタモデル

脅威は外側から
守るものは内側

クローズドな世界
（自分のところ）は
安全である

ゼロトラスト

脅威はあらゆる場所に

信頼の積み重ね

Security By Design

＋

サイバーハイジーン（公衆衛生）

全てのITの衛生管理を徹底
＜NISCや経団連も提唱(*)＞

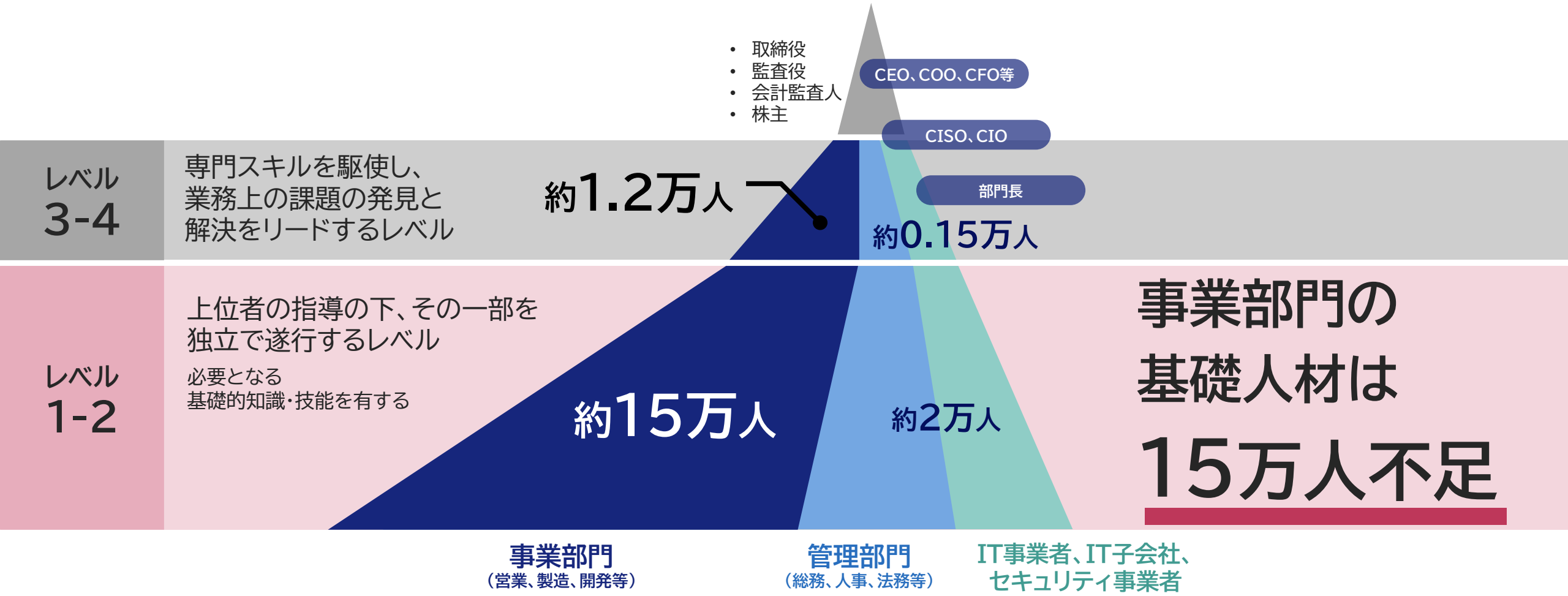
日常の運用で予防

Security Awareness

(*)サイバーセキュリティ意識・行動強化プログラム（内閣サイバーセキュリティセンター「NISC」）https://www.nisc.go.jp/active/kihon/pdf/awareness2019.pdf
Society5.0実現に向けたサイバーセキュリティの強化を求める（日本経済団体連合会） https://www.keidanren.or.jp/policy/2017/103_honbun.pdf

解消しないセキュリティ人材不足

セキュリティ人材不足数の各部門とスキルレベルとのマッピング



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/pdf/report/Human-Development-Plus-Security.pdf を元にNEC作成

サイバーハイジーン

日常におけるセキュリティ対策
エンドポイント・環境の衛生状態を維持する

管理者

- 情報持ち出しルールの徹底
- 社内ネットワークへの機器接続ルールの徹底
- 修正プログラムの適用
- セキュリティソフトの導入および定義ファイルの最新化
- 定期的なバックアップの実施
- パスワードの適切な設定と管理
- 不要なサービスやアカウントの停止または削除

ユーザー

- 修正プログラムの適用
- セキュリティソフトの導入および定義ファイルの最新化
- パスワードの適切な設定と管理
- 不審なメールへの注意
- USBメモリなどの取扱いの注意
- 社内ネットワークへの機器接続ルールの遵守
- ソフトウェア導入時の注意
- パソコン等の画面ロック機能の設定

家庭内

- 修正プログラムの適用
- セキュリティソフトの導入および定義ファイルの最新化
- 定期的なバックアップの実施
- パスワードの適切な設定と管理
- メールやショートメッセージ、SNSでの不審なURLへの注意
- 偽のセキュリティ警告に注意
- スマートデバイスのアプリや構成ファイル導入時の注意
- スマートフォン等の画面ロック機能の設定

情報処理推進機構　日常におけるセキュリティ対策

セキュリティ アウェアネス

セキュリティ・アウェアネス

- セキュリティに対する意識向上（気づき）
- 各自が IT セキュリティの問題を認識し、適切な対応を行うことを意図する
（NIST SP800-16）

Awareness≠Literacy

サイバーハイジーンを
実現するうえでのポイント

セキュリティ・アウェアネスを高める

リテラシー

- ある分野における知識や理解力
- 網羅的・体系的
- 技術的要素を含むことがある
- トレーニングでスキルを習得

アウェアネス

- ある事象における気づき・意識
- 事象にフォーカス
- 技術的要素は薄い
- 継続的気づきを得る体験

高度人材とアウェアネスでビジネスに勝つ


Orchestrating a brighter world
NEC