SEA/Jテキストで解説するセキュリティ知識は実社会でどう役立つのか？

～適切なセキュリティ対策をしていた「はず」が・・・なサイバーリスクから学ぶ～

日本ネットワークセキュリティ協会 (JNSA)
担当講師：齋藤実成

アジェンダ

１．基礎編テキストの改訂ポイント

２．今、どんな社会になっているだろうか？

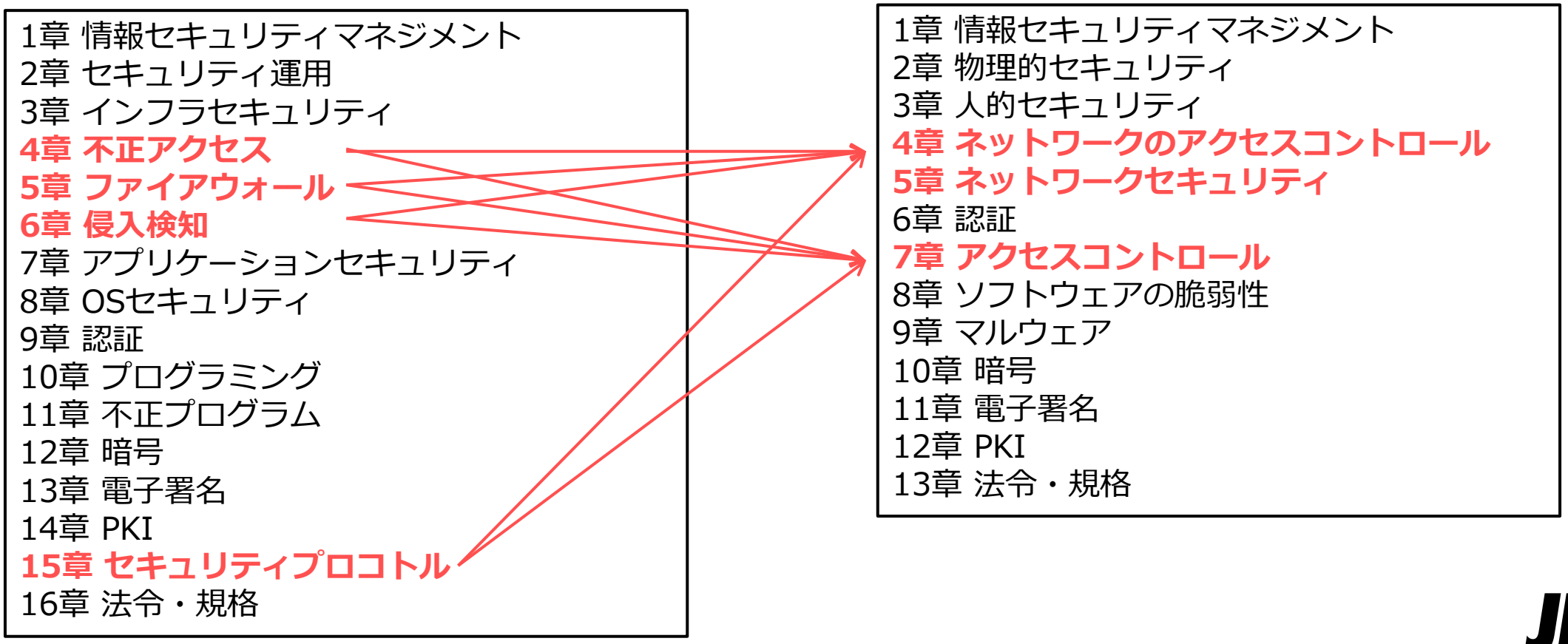
３．セキュリティ対策の困りごと

４．エッ、対策していても盗まれるんですか？（汗）

１．基礎編テキストの改訂ポイント

基礎編テキストの改訂ポイント　～ネットワーク・アクセスコントロール～

最新動向や技術書汎用構成を踏まえて、旧テキストにて各章に点在する項目を「ネットワークのセキュリティ知識」や「アクセスコントロール」として改廃



基礎編テキストの改訂ポイント　～ネットワーク・アクセスコントロール～

技術用語や技術・テクニック等を「基礎知識」として解説することに加えて、セキュリティ対策を「応用知識」として学べるよう再編成

・4章を「ネットワークのアクセスコントロール」として再編成
・5章を「ネットワークセキュリティ」として再編成
・7章を「アクセスコントロール」として再編成

【参考】4章構成(1)

4.1 ネットワークのアクセスコントロール

4.1.1 階層ごとのアクセスコントロール
4.1.2 パケットフィルタリング
4.1.3 ステートフルインスペクション
4.1.4 サーキットレベルゲートウェイ
4.1.5 アプリケーションゲートウェイ

4.2 ファイアウォール

4.2.1 ファイアウォールとは
4.2.2 フィルタリングルールの設計
4.2.3 DMZ の設計
4.2.4 ログ解析

JNSA

【参考】4章構成(2)

4.3 NAT

4.3.1 NAT（アドレス変換技術）

4.4 犯罪との関係（不正アクセスとの関係）

4.4.1 不正アクセスの目的

4.4.2 踏み台

【参考】 5章構成(1)

5.1 ネットワークを保護するためのセキュリティ技術 (1)

5.1.1 SSH (Secure Shell)

5.1.2 TLS (Transport Layer Security) / SSL (Secure Socket Layer)

5.1.3 IPsec

5.1.4 DNS の仕組み (名前解決の仕組み)

5.1.5 DNS のセキュリティ対策

5.1.6 無線 LAN における脅威

5.1.7 無線 LAN のセキュリティ対策

JNSA

【参考】5章構成(2)

5.2 ネットワークを保護するためのセキュリティ技術 (2)

5.2.1 IDS の概要

5.2.2 ネットワーク型 IDS

5.2.3 ホスト型 IDS

5.2.4 IDS の構成

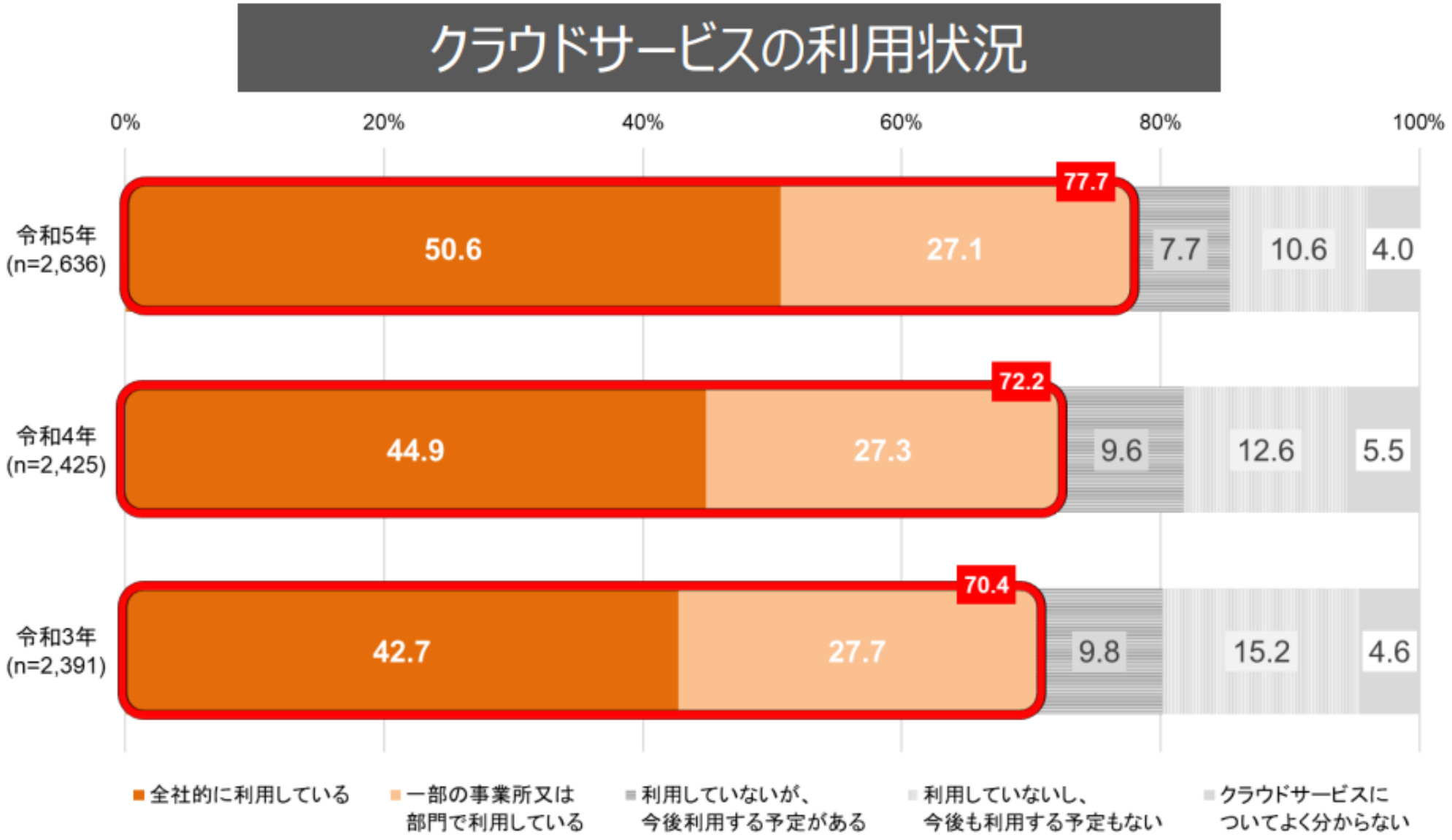
5.2.5 IPS (Intrusion Prevention System)

5.2.6 ハニーポット

２．今、どんな社会になっているだろうか？

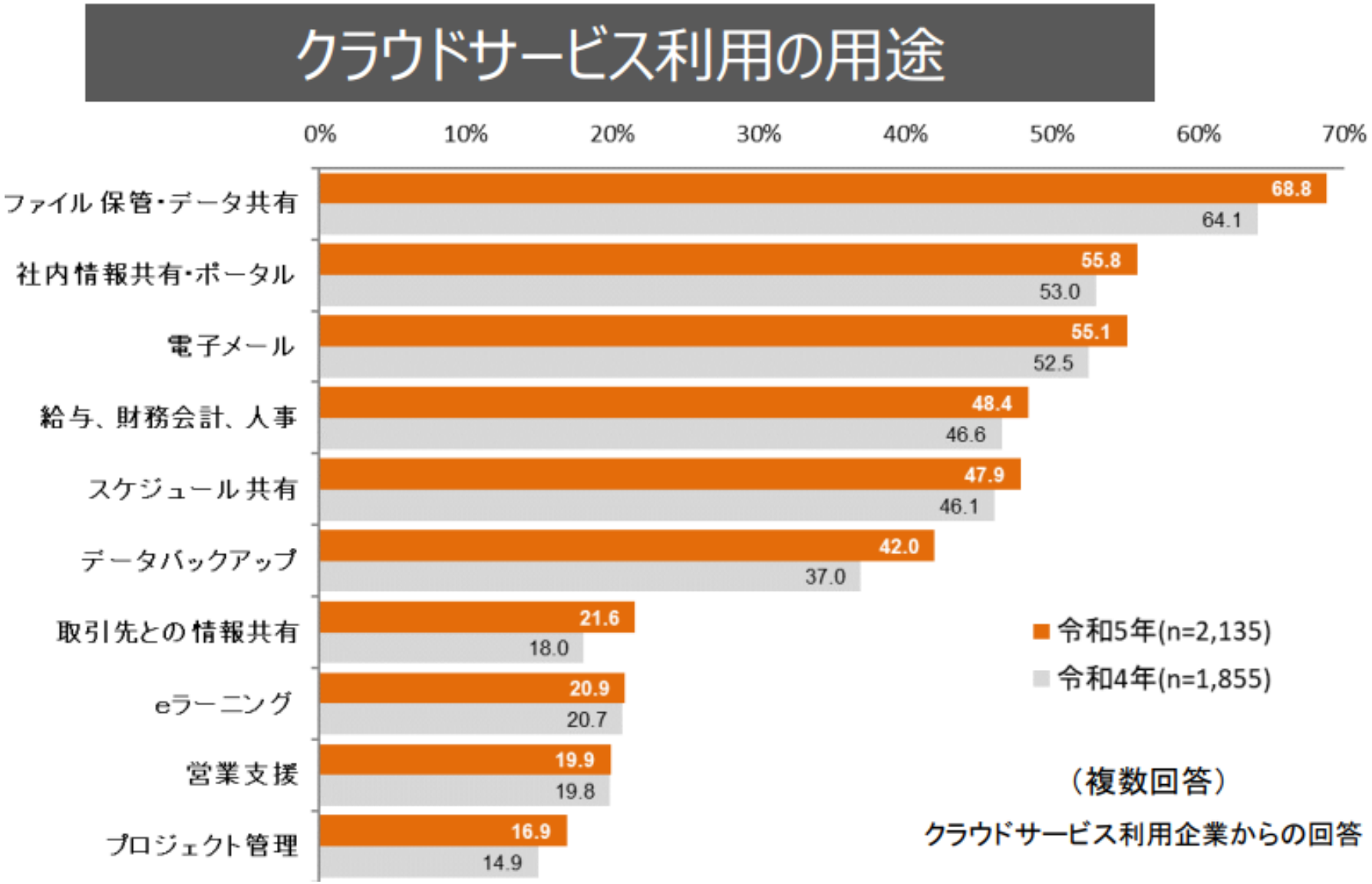
※出展：令和５年通信利用動向調査 - 総務省

クラウドサービスの利用状況



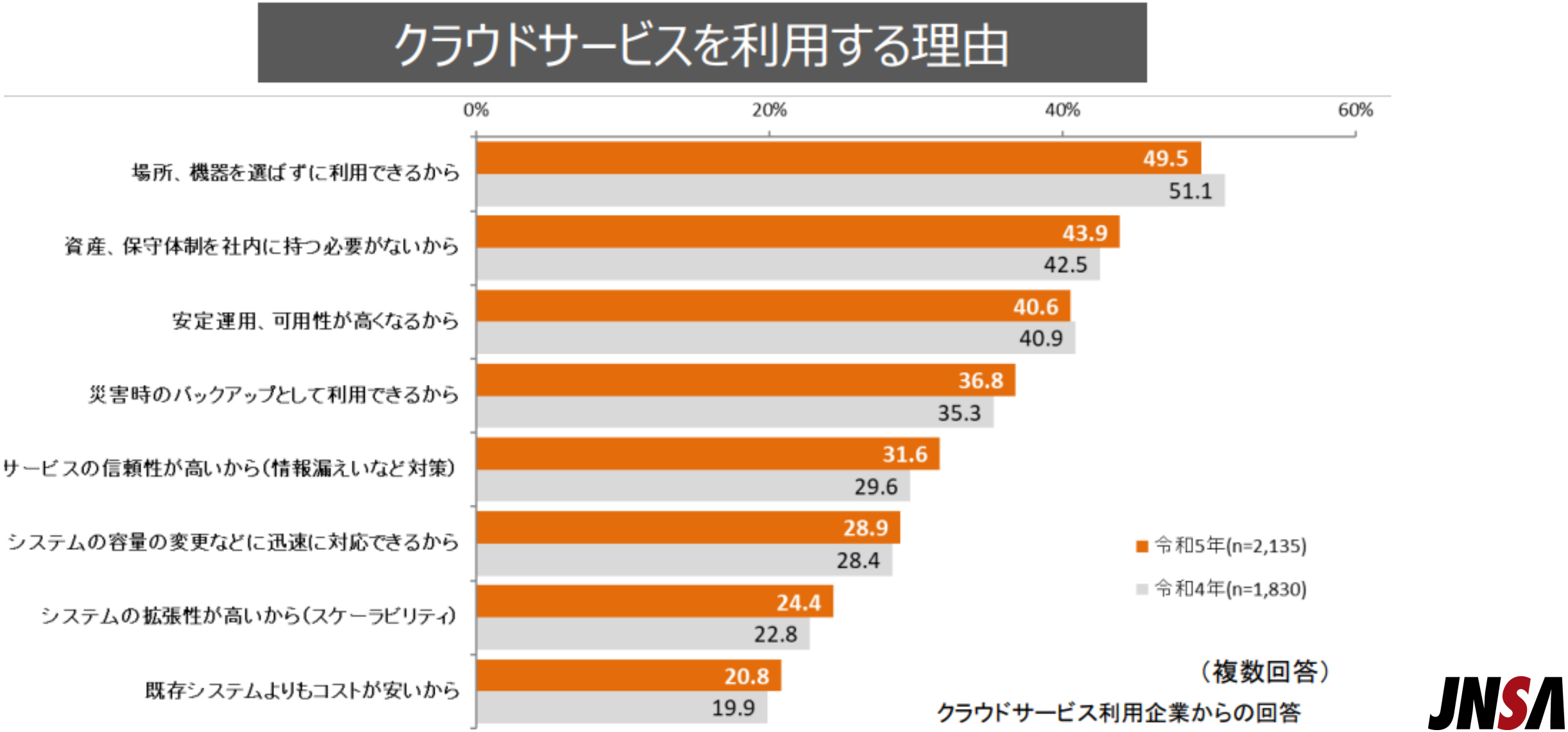
※出展：令和５年通信利用動向調査 - 総務省

クラウドサービスの利用用途



※出展：令和５年通信利用動向調査 - 総務省

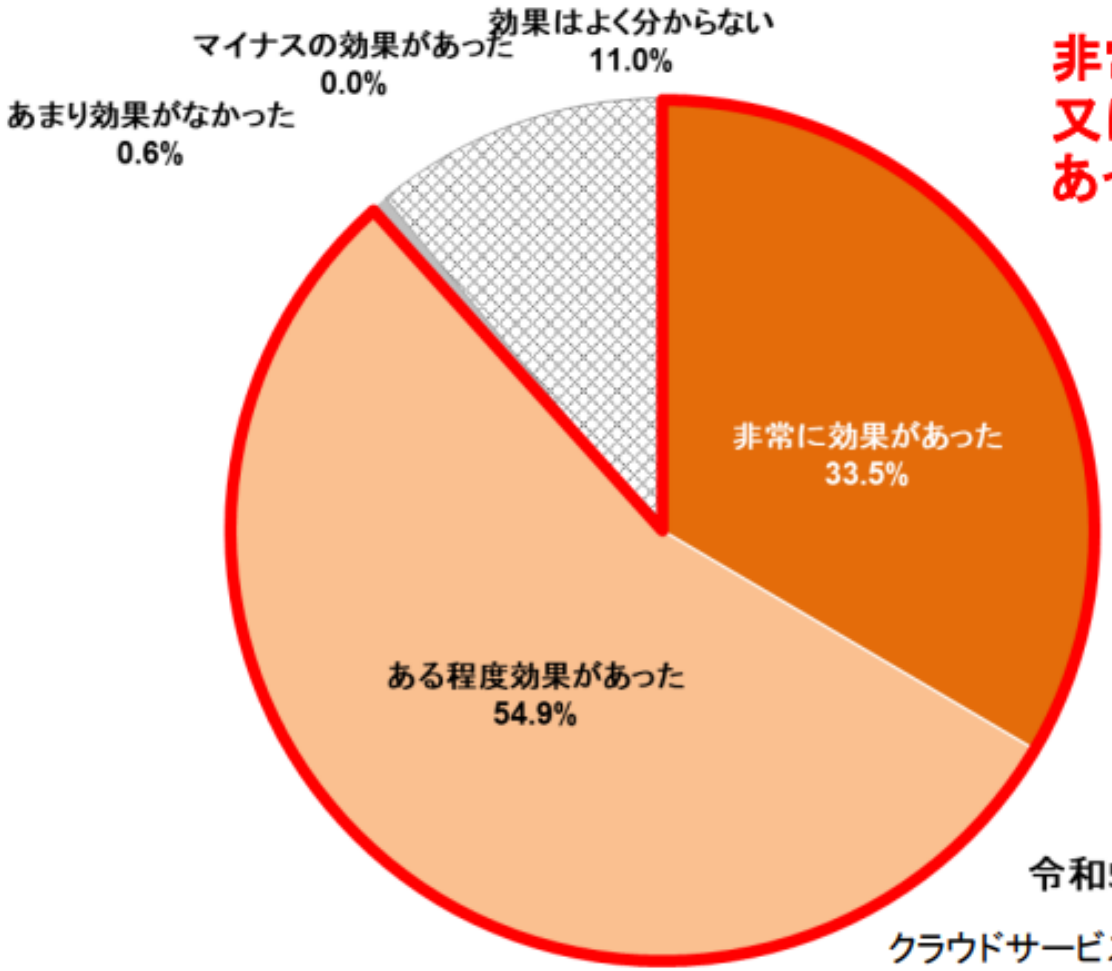
クラウドサービスを利用する理由



※出展：令和５年通信利用動向調査 - 総務省

クラウドサービスの利用効果

クラウドサービス利用の効果



非常に効果があった又はある程度効果があった　88.4%

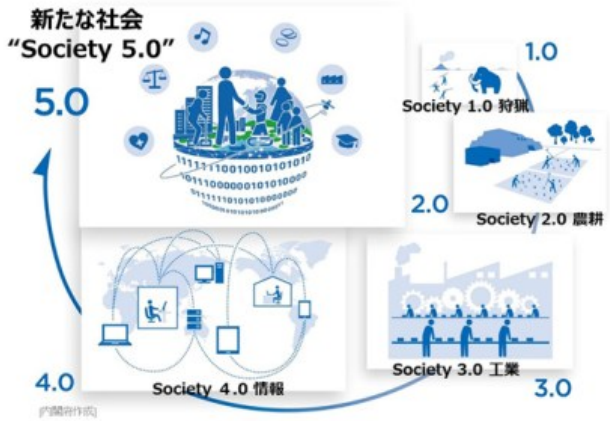
令和5年(n=2,126)

クラウドサービス利用企業からの回答

Society5.0の理想と闇

Society5.0によるフィジカル空間とサイバー空間の
高度な融合により、経済発展や社会課題の解決を後押し。

同時に、これまで「境目」があった脅威が空間を越境、
サイバー攻撃を受けた際の影響も深刻化。



内閣府Society 5.0「科学技術イノベーションが拓く新たな社会」説明資料

経団連policy　Society5.0　–ともに創造する未来-

JNSA

Society5.0の闇(具体例)

- ■物資運搬ドローン　→　書き換えられる配送先や地図
- ■ロボットや自動運転車　→　意図的な事故
- ■自動分析・自動制御　→　フェイクデータによる扇動

あらゆるものが繋がる世界になりつつあるが、
特に「**故意だった場合**」に対する考慮が不十分

人類の進化は道具の進化？(道具の活用と生活の変革)

- 200万年前、人は石器により自分たちよりも力の強い動物を狩って暮らすことができるように。
- 1万年前、土器により食料を貯えたり食料を調理できるように。
- 5,500年前には文字が、2,100年前には紙が生み出され、遠い昔の出来事を今に残すことができるように。

道具の二面性と効力

- 石器や鉄器は「武器」として有用だった
- 火は「火災事故の危険」と「武器」として活用
- 文字、紙、活版印刷は「世論操作や事実改ざん」にも
- 羅針盤は精度過信による「事故」や「故意に狂わせる」ことも
- コンピュータに至っては誕生背景からも「様々な脅威」を内包

「道具を使いこなす」とは、過去を省みるとどうも脅威をもたらす側面で
まず利用されていて、それから幸せのために使われているようだ。
また、道具を最も使いこなした者が世界・社会・時代をリードしてきた。

基本的には「善いことのために生まれる→悪いことに使われる→発展する」
そして「より良い社会のために使われる」

JNSA

Society5.0時代の「道具」とは？

では、
Society5.0時代の
「道具」とは
一体なんなのだろうか？

Society5.0時代の「道具」とは？

企業組織がこの時代を生き残るためには、
「道具を使い倒す」ということが必要になってくる。
・・・Society5.0における道具とはなんなのだろうか？

ポイントは

ソフトウェアとデータ

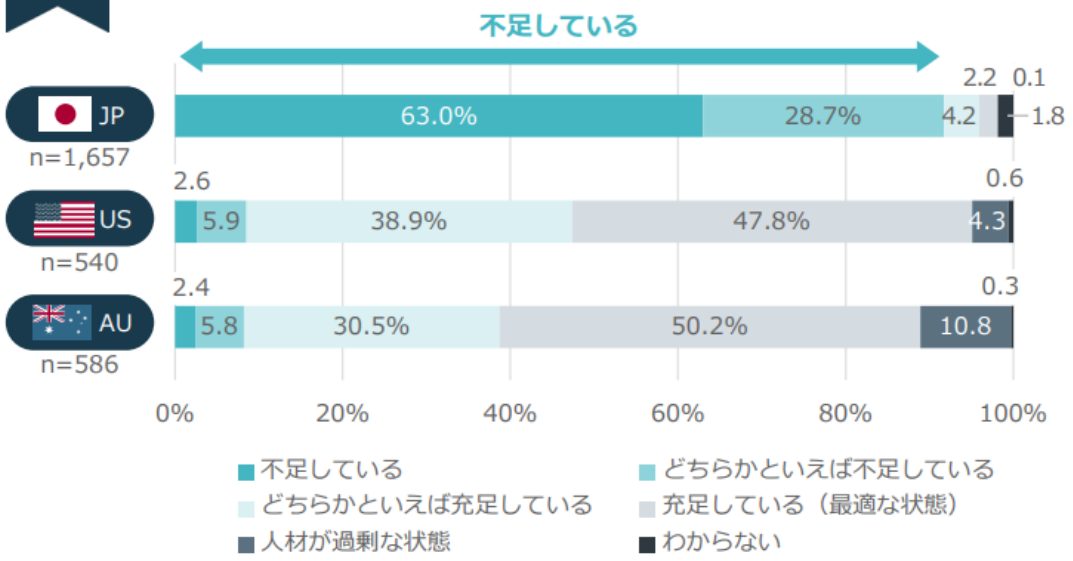
JNSA

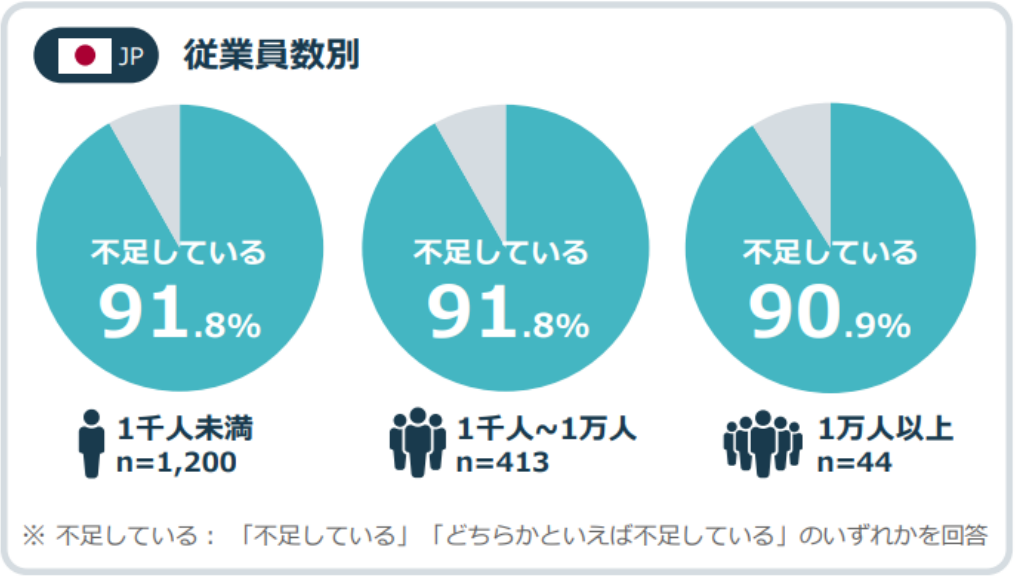
３．セキュリティ対策の困りごと

※出展：NRI Secure Insight 2023

セキュリティ人材

セキュリティ人材の充足状況





Key Results

セキュリティ人材が不足していると回答

JP 約90%

1千人未満 ＝ 1千人~1万人 ＝ 1万人以上

Key Insights

- 日本では約9割がセキュリティ人材が不足していると回答しており、慢性的な人材不足の傾向が10年以上続いている。企業規模による回答の差は見られず、日本企業の共通的な課題であることを示す結果となった。
- 少子高齢化の進行により、日本の生産年齢人口は減少している。また、DXの進展により、企業におけるセキュリティリスクは多様化・深刻化しており、セキュリティ人材の希少価値はさらに増している。
- セキュリティ人材不足を解消するために、人材の獲得・育成は依然として有効な打ち手であるが、その数は有限である。解消を後押しする補完策・代替策の検討や実践が欠かせない。

JNSA

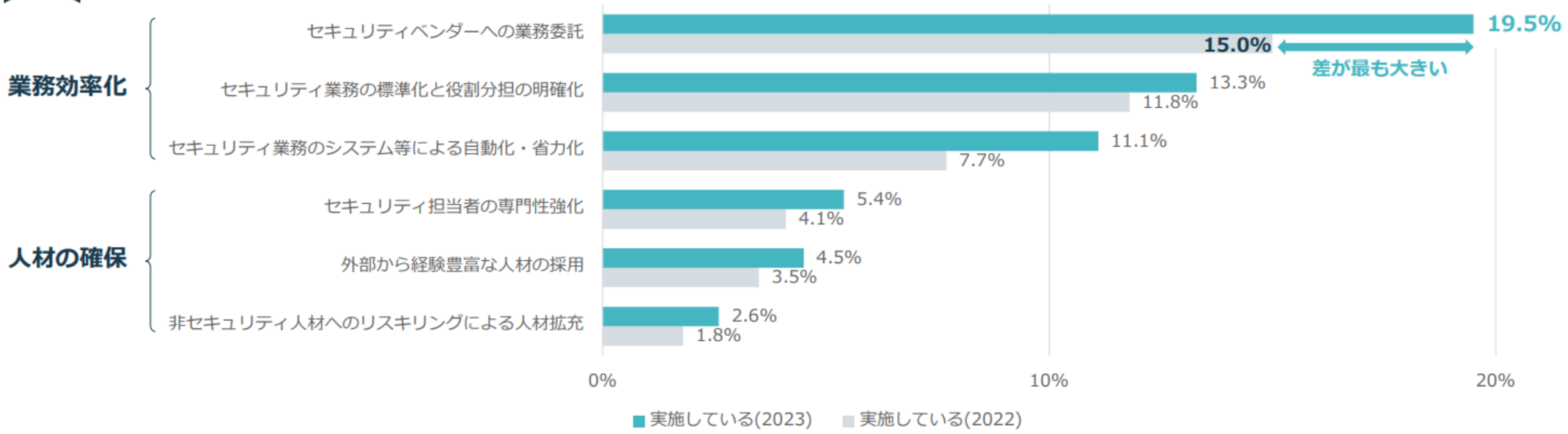
※出展：NRI Secure Insight 2023

セキュリティ人材不足を補う施策

「不足している」と回答した企業のセキュリティ人材不足を補う施策の実施状況

JP n=1,520

※ セキュリティ人材が不足している／どちらかといえば不足していると回答した企業のみ対象



Key Results

増加した施策（前年度比）

No.1	セキュリティベンダーへの業務委託	+4pt
No.2	セキュリティ業務のシステム等による自動化・省力化	+3pt

Key Insights

- 「セキュリティベンダーへの業務委託」はセキュリティ業務を効率的・効果的に実施する上で有効な選択肢であるが、サステナブルなセキュリティ活動を実現するためには、セキュリティ人材の確保やセキュリティ業務の効率化などの複数施策をバランスよく実践していくことが求められる。
- 実施率が最も高い業務委託の回答が2割弱に留まっている理由は、セキュリティ関連予算の不足や現場が常時繁忙で検討や実行の時間が取れないことなどが原因と推察する。人材不足の真の解消には、経営主導の積極的な予算確保などの配慮や現場の後押しが欠かせない。

※出展：NRI Secure Insight 2023

セキュリティ担当者の困りごと

企業のセキュリティ担当者として、最も対応に困っている事項

JP 従業員数別

※ 最大3つの複数選択可

	1千人未満 n=1,200	1千人～1万人 n=413	1万人以上 n=44
1位	39.5% セキュリティインシデント発生時の緊急対応	43.1% セキュリティ人材の育成	50.0% セキュリティ人材の育成
2位	37.3% サイバー攻撃の高度化への対応	41.2% セキュリティインシデント発生時の緊急対応	43.2% 業務委託先や取引先のセキュリティ統制・管理
3位	36.5% セキュリティ人材の育成	33.9% グループ会社・国内外拠点のセキュリティ統制・管理	29.5% サイバー攻撃の高度化への対応
4位	34.0% 自社セキュリティ対策の遅れ（最新技術・動向の未反映）	31.2% 自社セキュリティ対策の遅れ（最新技術・動向の未反映）	27.3% セキュリティインシデント発生時の緊急対応
5位	19.6% セキュリティ脅威・事故に関する情報収集と関係者共有	31.0% サイバー攻撃の高度化への対応	25.0% 自社セキュリティ対策の遅れ（最新技術・動向の未反映）

※ 他選択肢：セキュリティ業務の状況・進捗に関する経営層への報告 ／ セキュリティ対策のトレンド・他社動向の把握 ／ テレワーク環境におけるセキュリティの確保 ／ DX化に伴うデジタルサービスのリスク分析・把握 ／ その他（具体的に記載） ／ 困っていることはない

Key Results

IPA情報セキュリティ10大脅威※が上位の困りごとに影響と予想

- 10大脅威の1位 ランサムウェア
  - セキュリティインシデント発生時の緊急対応
  - サイバー攻撃の高度化への対応
- 10大脅威の2位 サプライチェーン攻撃
  - グループ会社・国内外拠点のセキュリティ統制・管理
  - 業務委託先や取引先のセキュリティ統制・管理

Key Insights

- 従業員数が1千人以上の企業では、人材育成とグループ会社や委託先の統制・管理に関する困りごとが上位にある。IPAの10大脅威の2位であるサプライチェーン攻撃に対応する一方で人材不足に拍車がかかっていると推察する。
- 1千人未満の企業の1位・2位にあるように、セキュリティの事前対策と事後対応への意識が高まっている。
- サプライチェーン攻撃では、規模の小さい企業も狙われるため、グループ会社や委託元からの統制は広範囲に及ぶ。1千人未満の企業は、その要請に対応することでセキュリティ意識がさらに高まることが予想される。

※参考　IPA『情報セキュリティ10大脅威 2023』
https://www.ipa.go.jp/security/10threats/10threats2023.html

JNSA

４．エッ、対策していても盗まれるんですか？（汗）

攻撃者視点で考える「侵入から攻撃」までの手口

1．情報収集
- ✓ 攻撃対象への侵入に必要な情報を収集し、攻撃先と手法と特定
- ✓ ここで収集する情報は、単なるシステム情報に限らない

2．侵入
- ✓ 収集した情報に基づき、確実かつ気付かれずに攻撃対象へ侵入

3．攻撃活動
- ✓ 例：情報窃取 / 遠隔操作 / DDoS攻撃等の活動を展開

4．継続活動
- ✓ さらなる攻撃活動を継続するため、バックドアの設置やC2サーバとの通信を秘匿して確立（組織立って行われることが多い）

JNSA

攻撃活動の具体例

例１．情報窃取

✓ 組織や企業の機密情報や、顧客から預かっている個人情報などを狙い、侵入後にどのような情報があるのかシステム内を探索する。

例２．遠隔操作

✓ さらなる情報の探索や、詳細なアカウントや業務の情報を収集を目的に、社員の端末をマルウェア感染させることで遠隔操作を実現する。

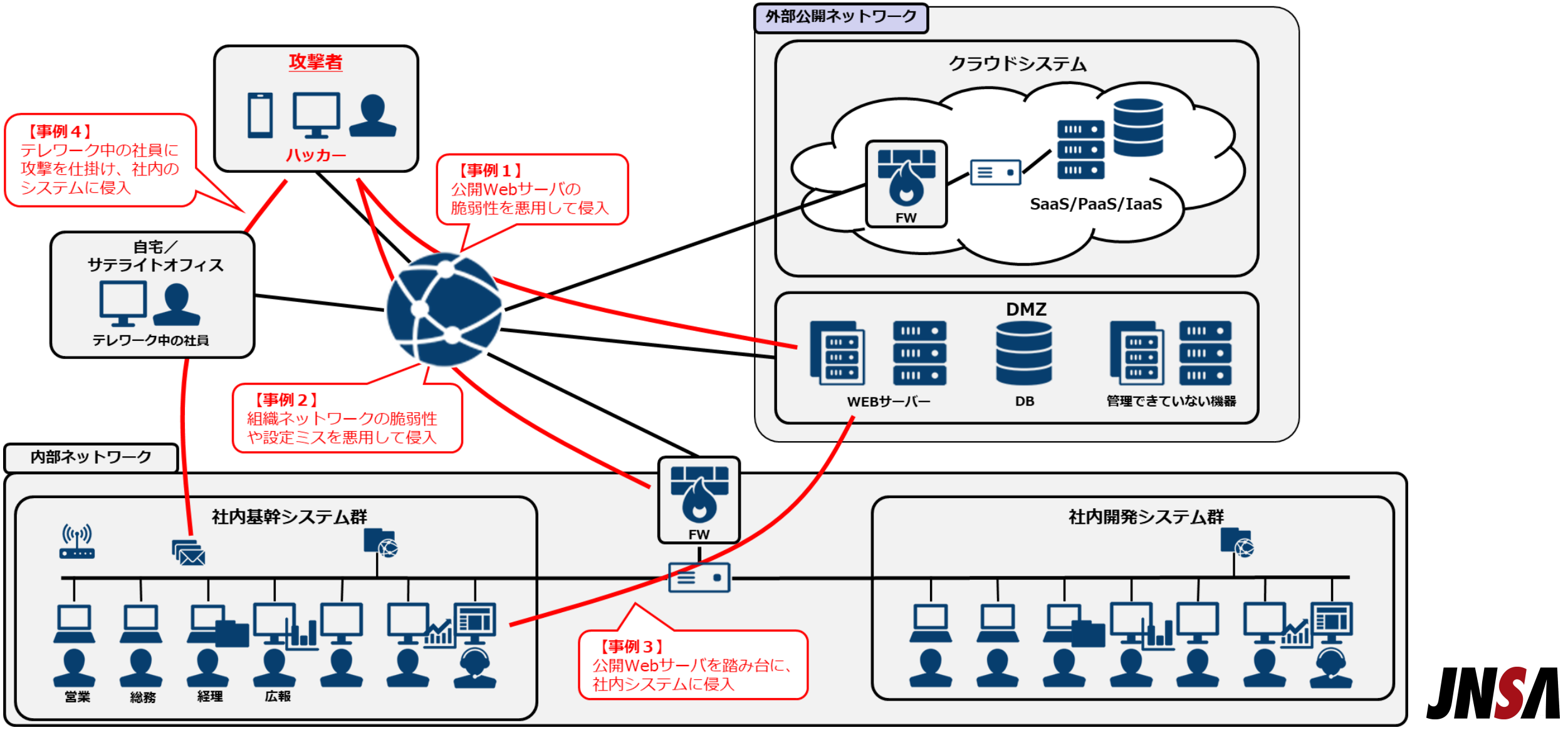
例３．DDoS攻撃 / DoS攻撃

✓ 提供するサービスを妨害するために、攻撃対象のシステム（サーバ）へ大量のデータを送りつける。

✓ 特定の宗教や思想に基づく攻撃も多く、思想に基づく攻撃を行うようなハッカーは、一般に「ハクティビスト」と呼ばれている。

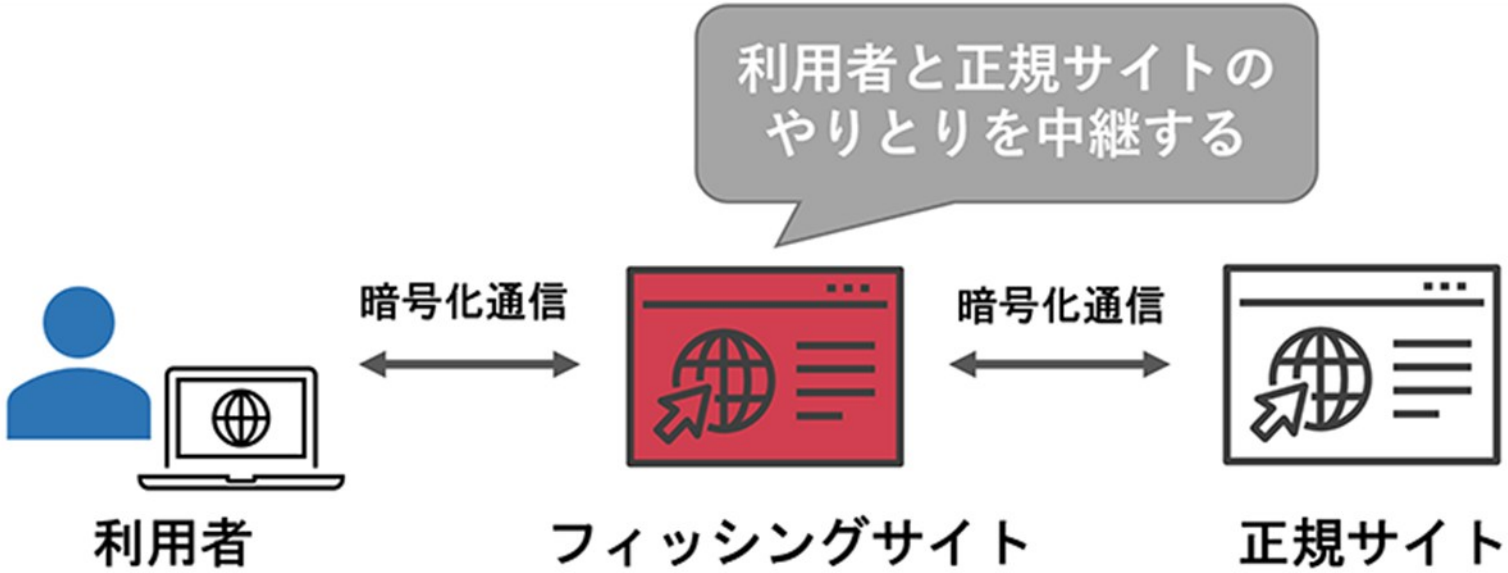
JNSA

【参考】侵入手法の具体例


攻撃者
ハッカー
【事例４】
テレワーク中の社員に
攻撃を仕掛け、社内の
システムに侵入
【事例１】
公開Webサーバの
脆弱性を悪用して侵入
自宅／
サテライトオフィス
テレワーク中の社員
【事例２】
組織ネットワークの脆弱性
や設定ミスを悪用して侵入
外部公開ネットワーク
クラウドシステム
FW
SaaS/PaaS/IaaS
DMZ
WEBサーバー
DB
管理できていない機器
内部ネットワーク
FW
社内基幹システム群
営業
総務
経理
広報
社内開発システム群
【事例３】
公開Webサーバを踏み台に、
社内システムに侵入

フィッシング攻撃は多要素認証を突破するようになってきている

フィッシングサイトが正規サイトの中継役に



フィッシング攻撃からID・パスワード等のアカウント情報を保護するためには、
他要素認証(MFA)が有効。

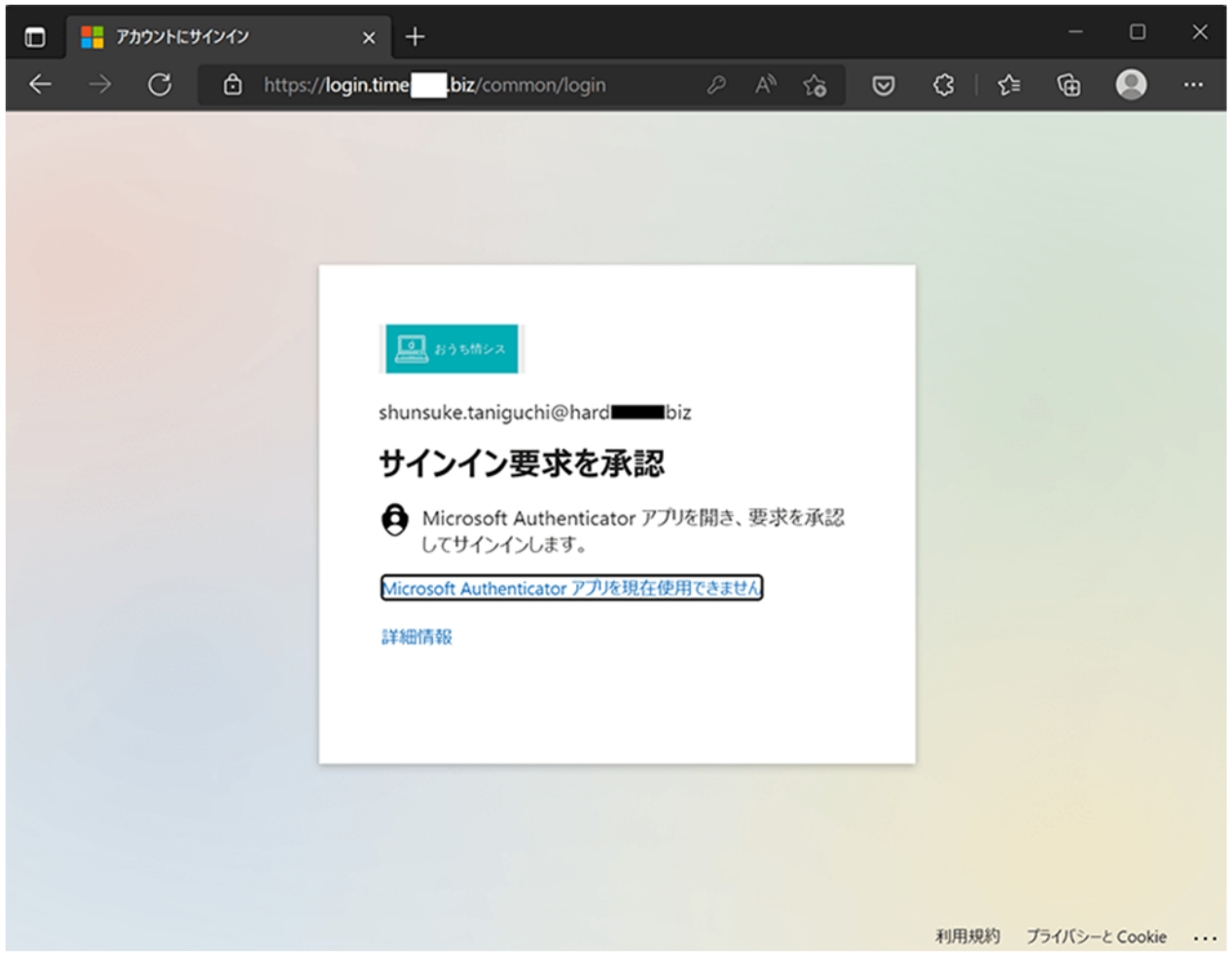
しかし、最近は**利用者を騙して**MFAの承認を**不正中継**する攻撃手法が登場。

過去には**ワンタイムパスコードを同様の手法で盗難**する攻撃も存在、注意しておきたい。

JNSA

フィッシング攻撃は多要素認証を突破するようになってきている

Evilginx2を用いてプロキシサーバとして動作するフィッシングサイト
※GitHubに公開されているツール



出典：多要素認証（MFA）だけでは守れないフィッシング攻撃の対策(ラック)より抜粋
https://www.lac.co.jp/lacwatch/report/20220909_003103.html

- ✔ 利用者が**騙されてID・パスワードを入力**すると、その後の**MFAの要求画面**が利用者に転送される。
- ✔ MFAは正規サイトのものであるため、利用者が**気付かず承認**してしまった場合、フィッシングサイト経由で認証成功後の**Cookie情報が盗難**されてしまう。
- ✔ これらのフィッシング攻撃は、**AiTM (Adversary in The Middle)**と呼称される。
- ✔ 対策手法としては、**ゼロトラストセキュリティのアーキテクチャ**を採用したシステム基盤の構築(MDMによるポリシー適用)等が挙がる。
- ✔ 当該攻撃手法は、企業所属者だけでなく**一般利用者に対する攻撃**としても活用可能。

JNSA


JNSA