情報セキュリティツール活用研修 ［決定版］

～すぐに役立つツールで実践する、本当に効く情報セキュリティ対策～

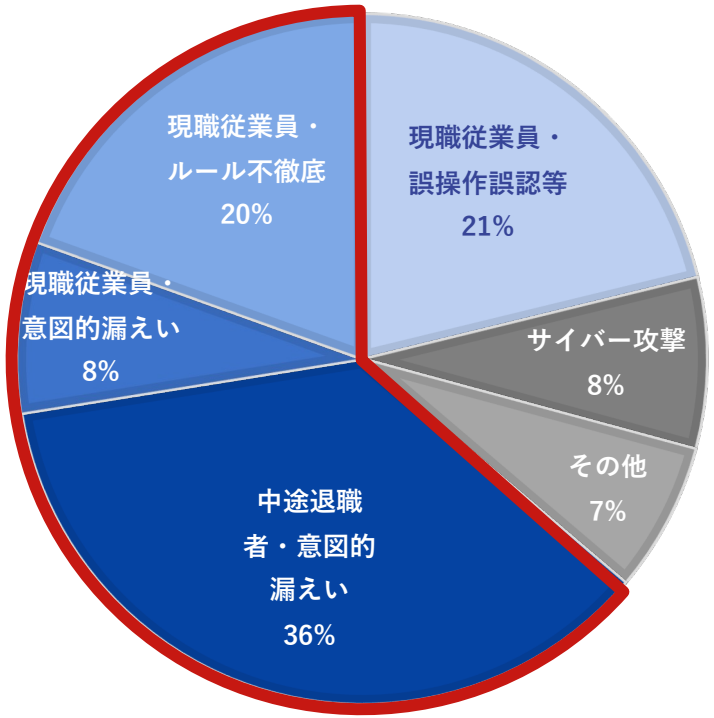
サイファ・コア 株式会社

2024.11.27

情報漏えいに関する実態

従業員を通じた情報漏えいは 8 割 超！

企業にとって従業員への情報セキュリティ教育が急務です



6 4 %がルール未遵守による漏えい

4 4 %が意図的な漏えい

（中途退職者および現職従業員から）

図：IPA「企業における営業秘密管理に関する実態調査 2020 調査実施報告書」をもとに当社作成

秘密情報の安全管理は重大な経営課題 (1)

経営者の引責辞任、行政指導につながる個人情報漏えい

朝日新聞デジタル ＞ 記事

NTT西日本の森林社長が辞任表明　個人情報の大量流出問題で引責

金子智彦　2024年2月29日 16時07分

記者会見の冒頭でおわびし、頭を下げるNTT西日本の森林正彰社長（中央）と、子会社2社の社長と

NTT西日本の子会社の元派遣社員が約900万件の個人情報を不正流出させた問題で、NTT西の森林正彰社長は29日、3月末に引責辞任すると表明した。森林氏は同日の記者会見で「多くのみなさまに多大なご迷惑をおかけした。社会的責任は重大」と述べた。後任は「しかるべきタイミング」で発表するとした。

Source：朝日新聞デジタルより

日本経済新聞

朝刊・夕刊　LIVE　Myニュース

トップ　速報　オピニオン　経済　政治　ビジネス　金融　マーケット　マネーのまなび　テック　国際　スポーツ

LINEヤフー行政指導へ　総務省、情報漏洩相次ぎ

2024年3月1日 2:00 [会員限定記事]

保存

総務省は近く不正アクセスによる情報漏洩を相次ぎ公表したLINEヤフーを行政指導する。LINEアプリを巡るセキュリティーガバナンスや業務委託先の監督などの強化を要求する。利用者利益を保護するために改善策の実施状況の報告も求めていく。（**関連記事経済・政策面に**）

大株主である韓国ネット大手ネイバーと事実上一体で運用されている安全性への配慮に欠くシステム管理の是正を促す。特にLINEとネイバーのサーバーにアクセスするための一部システムの認証基盤が共通になっている点を問題視した。

こうした運用が情報漏洩を招いたとしてシステムの早期分離などの改善を求める。LINEヤフーは経済安全保障推進法で特定社会基盤事業者に指定されており、経済安保の観点からもリスク管理を強化させる。

Source：日本経済新聞電子版より

秘密情報の安全管理は重大な経営課題 (2)

転職者による営業秘密情報の持ち出しが年々増加

かっぱ寿司社長逮捕「迂闊な引き抜き」への警告
前勤務先の営業秘密流出はどれほど危ない行為なのか

1 2 3 4 5

坂口 孝則：調達・購買業務コンサルタント、講演家　＋ 著者フォロー　2022/10/01 10:59

シェアする　ポストする　ブックマーク　メールで送る　印刷　A+ 拡大　A− 縮小

かっぱ寿司をめぐる事件が指し示す企業リスクとは？（撮影：今井 康一）

回転寿司チェーン「かっぱ寿司」を運営するカッパ・クリエイトの田邊公己社長（46）が警視庁に逮捕された。

容疑は不正競争防止法違反だ、田邊氏はかつて同業である「はま寿司」の親会社となるゼンショー（現ゼンショーホールディングス）へ1998年に入

Source：東洋経済オンラインより

※警察庁によると、営業秘密侵害事犯は2013年以降増加で推移している

（「令和4年における 生活経済事犯の検挙状況等について」より）

朝日新聞 DIGITAL　能登半島地震　ウクライナ情勢　速報　朝刊

トップ　社会　経済　政治　国際　スポーツ　オピニオン　IT・科学　文化・

朝日新聞デジタル ＞ 記事

増える転職者、情報持ち出しで摘発事例も　企業の営業秘密・個人情報

有料記事

御船紗子　2023年9月15日 15時00分

警視庁本部

今回の事件で転職先へ持ち出されたのは、数万人の名刺情報だった。

企業独自の生産・販売方法といった 営業秘密 を転職先に持ち出すと、 不正競争防止法 違反に問われる可能性があるが、名刺情報は同法違反に当たらない。ただ警視庁は、名刺に記載された営業先の氏名、企業、役職や連絡先などは、 個人情報保護法 で定める個人情

Source：朝日新聞デジタルより

秘密情報の安全管理は重大な経営課題 (3)

漏えい事故の損害額は、中小企業であっても 数千万円～数億円 単位

損害の種類		中小企業における損害額概算
事故対応損害	1.原因・被害範囲調査費用、2.コンサルティング費用、 3.法律相談費用、4.広告・宣伝活動費用、 5.コールセンター費用、6.見舞金・見舞品購入費用、 7.ネット炎上防止費用、8.ダークウェブ調査費用 9.クレジット情報モニタリング費用、10.超過人件費、 11.システム復旧費用、12.再発防止費用 など	**3,500万円～ ≒1億円**
賠償損害	1.損害賠償金、2.弁護士費用 など	**数百～数千万円以上**
利益損害	1.数ヶ月の売上高の減少、2.固定費の支払い など	**売上高や固定費に比例**
金銭損害	ランサムウェアによる身代金	**数千万円以上**
行政損害	個人情報保護法上の罰金	**最大1億円**
無形損害	1.顧客離れ、2.株価下落 など	**換算不能な損失**

中小企業を想定した具体的な損害額 概算 /インシデント1件あたり

出典：NPO法人日本ネットワークセキュリティ協会(JNSA)「インシデント損害額調査レポート 第2版」 (https://www.jnsa.org/result/incidentdamage/data/2024-1.pdf)

秘密情報の安全管理は重大な経営課題(4)

情報流出によって大きな損害を出してしまった会社の事例

B 社	2014年6月、約2,895万件もの個人情報が名簿会社に売却されていた。 会員への補償のためにかかった**損害は260億円**、 2016年3月期連結決算の**最終損益は82億円の赤字**
N 機構	2015年５月、不正アクセスによって約125万件の情報が流出。 この事件を逆手に取った詐欺事件も発生し、**機構の信頼は失墜**
J社	２０１６年６月、オンラインサービスから７９３万件の個人情報が流出。 流出したパスポートの再発行の費用 **約７０００万円** 被害者からの訴訟も含めて**４０億円以上の補償**
A社	2015年2月、米国第2位の医療保険会社A社の8000万人の個人情報が流出。 氏名、生年月日、加入者ID、社会保障番号、住所、電話番号、電子メール アドレス、勤務先などの情報が流出し、**被害総額は100億円以上**

Source：【事例】個人情報流出で損失を出してしまった5つの経営ケース (株)エステイエス 経営コラム
https://web.all-in.xyz/upgrade/cybersecurity/

なぜ、インターネット上の情報漏えいが起こり続けるのか？

備えるべきセキュリティ機能を欠いたまま使われ始め、使い続けているから

1980年代初頭

脆弱性ある暗号を用い、機密性が確保されないまま利用開始

改善されず...
完全なセキュリティ機能は装備されず...

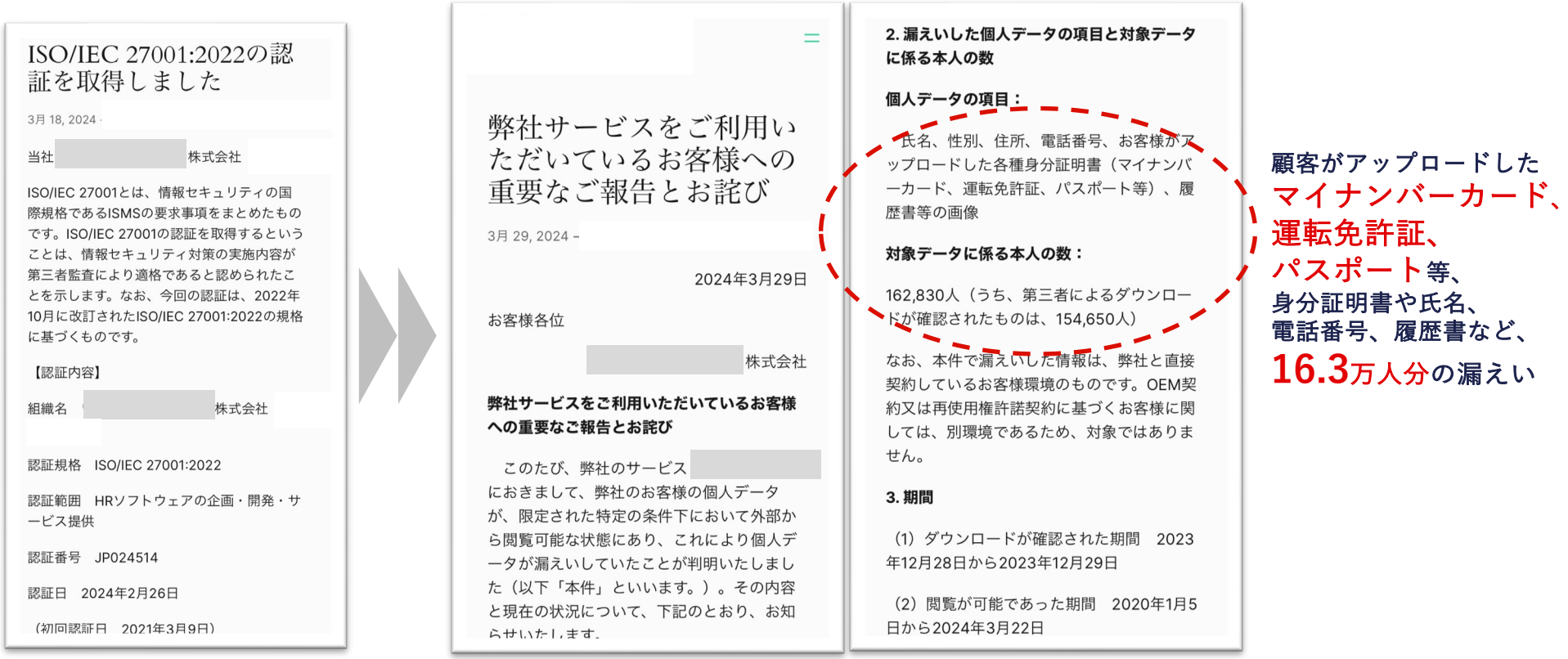
現在

不完全な暗号技術を用いる多くのサービスを、情報を守るスキルが乏しい人々が利用している

情報漏えいが後を絶たない理由 (1)

形骸化している情報セキュリティ認証および情報セキュリティ対策

ISMS認証 (※)を取得している企業でも、重大な情報漏えいを起こしている



ISO/IEC 27001:2022の認証を取得しました

3月 18, 2024

当社 株式会社

ISO/IEC 27001とは、情報セキュリティの国際規格であるISMSの要求事項をまとめたものです。ISO/IEC 27001の認証を取得するということは、情報セキュリティ対策の実施内容が第三者監査により適格であると認められたことを示します。なお、今回の認証は、2022年10月に改訂されたISO/IEC 27001:2022の規格に基づくものです。

【認証内容】

組織名 株式会社

認証規格　ISO/IEC 27001:2022

認証範囲　HRソフトウェアの企画・開発・サービス提供

認証番号　JP024514

認証日　2024年2月26日

（初回認証日　2021年3月9日）

弊社サービスをご利用いただいているお客様への重要なご報告とお詫び

3月 29, 2024 -

2024年3月29日

お客様各位

株式会社

弊社サービスをご利用いただいているお客様への重要なご報告とお詫び

このたび、弊社のサービス におきまして、弊社のお客様の個人データが、限定された特定の条件下において外部から閲覧可能な状態にあり、これにより個人データが漏えいしていたことが判明いたしました（以下「本件」といいます。）。その内容と現在の状況について、下記のとおり、お知らせいたします。

2. 漏えいした個人データの項目と対象データに係る本人の数

個人データの項目：

氏名、性別、住所、電話番号、お客様がアップロードした各種身分証明書（マイナンバーカード、運転免許証、パスポート等）、履歴書等の画像

対象データに係る本人の数：

162,830人（うち、第三者によるダウンロードが確認されたものは、154,650人）

なお、本件で漏えいした情報は、弊社と直接契約しているお客様環境のものです。OEM契約又は再使用権許諾契約に基づくお客様に関しては、別環境であるため、対象ではありません。

3. 期間

（1）ダウンロードが確認された期間　2023年12月28日から2023年12月29日

（2）閲覧が可能であった期間　2020年1月5日から2024年3月22日

顧客がアップロードした
マイナンバーカード、
運転免許証、
パスポート等、
身分証明書や氏名、
電話番号、履歴書など、
16.3万人分の漏えい

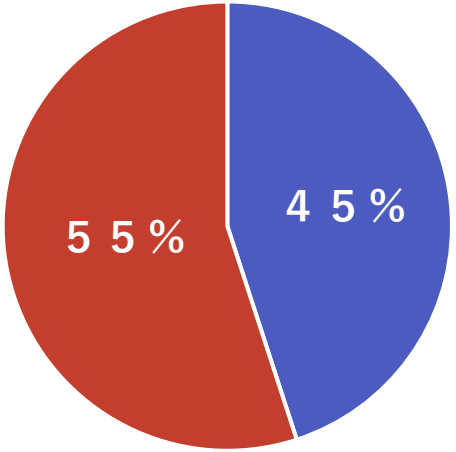
※ 情報セキュリティマネジメントシステムに関する国際規格 ISO/IEC 27001

Source：株式会社HPより

情報漏えいが後を絶たない理由 (2)

クラウド上の大量の機密データは暗号化されていない

暗号化されていない



一般的な暗号化（拙劣な暗号化を含む）

機密データが暗号化されているケースは平均 45%
2023年クラウドセキュリティ調査
(Thales Group)による

サービス事業者による対策への依存、既存の情報セキュリティ認証による判別には懸念

事業者任せでは不十分

自社内で対応できる施策はしっかり講じておくことで、情報保護の実効性が向上

情報漏えいが後を絶たない理由 (3)

時間稼ぎに頼る現在(標準)の暗号技術では、守れないのは明らか

コンピューティングパワーの増強 → **数時間・・・数分・・・数秒で解読**

量子コンピューターの実用化 → **一瞬で解読**

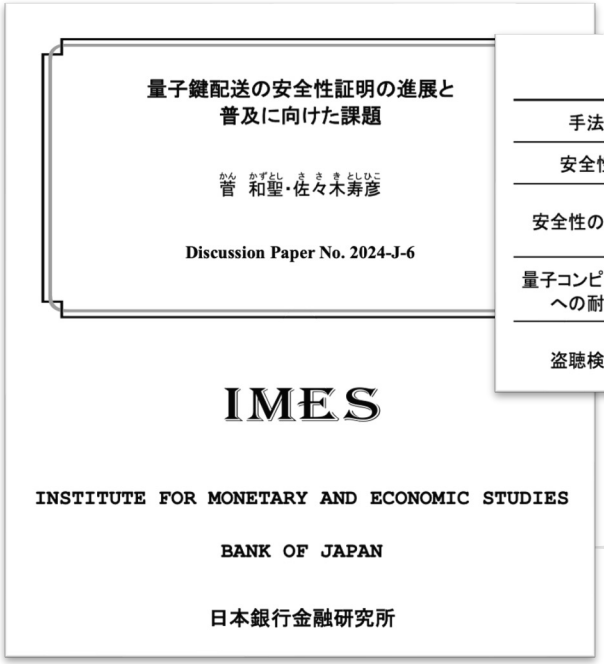
今後の動きとして、量子コンピュータの実現可能性の動向にかかわらず、より早期に、より強力な暗号に移行していくことが見込まれている

強力な暗号技術とは？

情報理論的安全性（※）に基づく暗号技術

将来的なコンピュータの能力向上や暗号解読アルゴリズム及び盗聴技術の進歩の影響を受けることがないため、無期限で通信内容の秘匿性を確保できる

（※ 攻撃者が無限の計算能力を有している場合や盗聴が行われる場合にも保証される強力な性質）


量子鍵配送の安全性証明の進展と
普及に向けた課題

菅 和聖・佐々木寿彦

Discussion Paper No. 2024-J-6

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

	RSA暗号、楕円曲線暗号（RSA、ECC）	耐量子計算機暗号（PQC）	量子鍵配送（QKD）
手法	公開鍵暗号	公開鍵暗号	量子暗号通信
安全性	計算量的安全性	計算量的安全性	情報理論的安全性
安全性の原理	素因数分解問題等の求解困難性	NP困難問題の求解困難性(注1)	量子力学的性質（物理法則）
量子コンピュータへの耐性	×	△	○
盗聴検知	×	×	○

- **現在、インターネットにおいて標準的に利用される暗号は、量子コンピュータによって効率的に解読されてしまう**
- **情報理論的安全性は、量子コンピュータによる暗号解読の脅威に対しても安全である**
- **しかしながら、情報理論的安全性に基づく　量子鍵配送は、未だ発展途上の技術**　(実証実験が進展中)

出典：日本銀行金融研究所「量子鍵配送の安全性証明の進展と普及に向けた課題」より

実用的な“ 情報理論的安全性に基づく暗号技術 ”

完全暗号 （サイファ・コアの独自技術）

相手を正確に認証した上で暗号鍵を配送することなく暗号通信し、情報理論的安全性を担保できる、最も実用的かつ安全な技術

	RSA暗号 楕円曲線暗号	耐量子計算機 暗号	量子鍵配送	**完全暗号**
手法	公開鍵暗号	公開鍵暗号	量子暗号通信	**暗号鍵を配送しない**
安全性	計算量的安全性	計算量的安全性	情報理論的安全性？	**情報理論的安全性**
安全性の原理	素因数分解問題等の求解困難性	NP困難問題の求解困難性	量子力学的性質（物理法則）	**情報理論**
量子コンピュータへの耐性	×	△	○	◎
盗聴検知	×	×	○	**必要なし**
実装容易性	◎	○	×	○
安価なコスト	◎	○	×	○

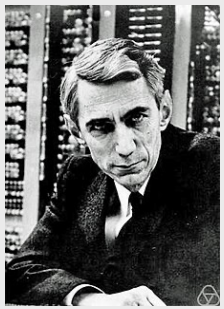
出典：日本銀行金融研究所「量子鍵配送の安全性証明の進展と普及に向けた課題」を参照し、当社作成

完全暗号 “COMPLETE CIPHER” の系譜

今世紀に完成した、論理的に解読不可能な暗号技術

完全な秘匿通信が可能となった

Claude Elwood Shannon



完全近接認証

完全秘匿保管

MIT(米国マサチューセッツ工科大学大学院元教授
コンピューター、情報通信、暗号、
人工知能等など今日の情報社会の基礎を作った

2つの技術を証明
in 1949

完全秘匿通信

完全遠隔認証

Takatoshi Nakamura

MIT(米国マサチューセッツ工科大学大学院) 元客員研究員
情報セキュリティ研究所 代表理事
サイファ・コア株式会社 CEO
人工知能、暗号、デジタル貨幣等を研究開発した

既存の2つを拡張 ＋ 残り2つの技術を発明
100% 完成　in 2005

「完全暗号」政府関係部門へ認知 in Japan

～ジャパン・レジリエンス・アワード 2024 ～ 最優秀賞を受賞

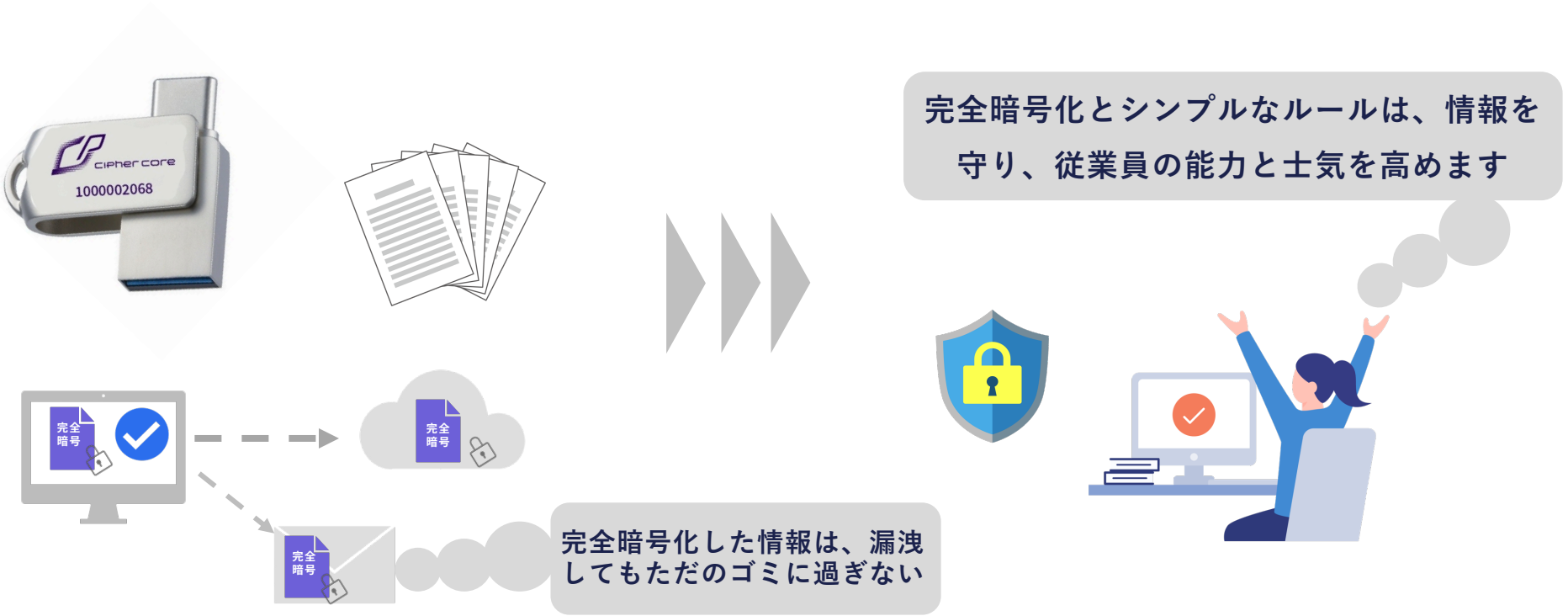
ジャパン・レジリエンス・アワード 2024

内閣官房国土強靭化推進室が取り組む、国土強靭化活動を行う組織の表彰において、
サイファ・コアの完全暗号技術を用いた通信網の構築が、最優秀賞を受賞

形だけの対策から、本物の「情報セキュリティ対策」へ！

政府は量子コンピュータとAIの脅威を認識し、対策を進めていく方針です。
当社はその解決策として、安全な機密情報管理の恩恵をあらゆる組織に享受頂くために、

今まで特別な機関にしか提供されてこなかった完全暗号を用いた
暗号化ツール “Cipher Key” を提供し、その使い方を教育します。



Cipher Key について

・暗号化アルゴリズムとして情報理論的安全性に基づいた完全暗号を使用している、サイファ・コア社独自の高度な暗号化ツールです。

・Cipher Keyによる高度な暗号化の際に入力する文字列は、一般的な暗号化ツールとは区別し、「Shadow Passcode」と呼びます。

ツール	情報秘匿方法	情報秘匿のために入力する文字列	暗号鍵	独自性	堅牢性
Cipher Key	**情報理論的安全性に基づく完全暗号化**	**シャドー・パスコード**	**ユーザ自身が提供する情報を含む複数の情報を用いて、都度異なる鍵を生成し使用する**	◎	◎
一般的なファイル暗号化	計算量的安全性に基づく暗号化	パスコード	予め用意された鍵の使い回し or 簡易的に生成される鍵を使用	△	○
パスワードロック	ファイルを開く際にパスワードで判断(※)	パスワード	なし	×	×

※ 中身は平文のままなので、解読しなくても内容を見ることができる

情報セキュリティの考え方

「情報そのものを守る」

本質を理解すれば、シンプルなツールで情報は守れます。

1. 情報の出入口ではなく情報そのものを守る。

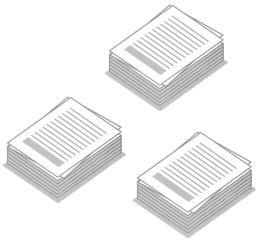
2. 耐量子コンピュータ対策には情報理論的安全性に基づく完全暗号を使用する

高度なレベルの機密情報 • 数年以上秘匿しておきたい情報 • 漏洩した場合の損害が多大になる情報	情報理論的安全性に 基づく完全暗号で守る
通常レベルの機密情報	一般の暗号で守る

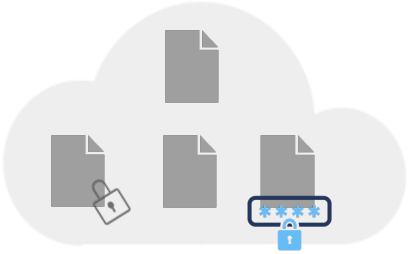
従来の対策

DXに伴い取り扱う情報量が増加し、多様なツールやプラットフォームが導入される中、

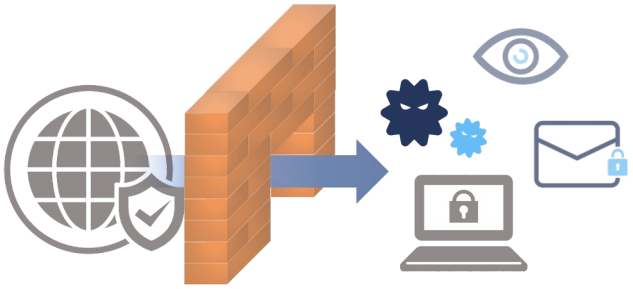
どんなに規程を増やしても、防御しても、漏えいが防げない



複雑・膨大な
組織規程



クラウドサービス事業者への
セキュリティ対策依存

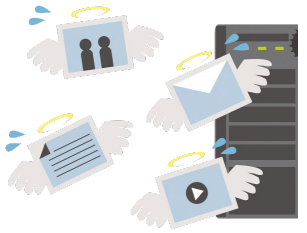


不完全な防御

疲弊

非効率

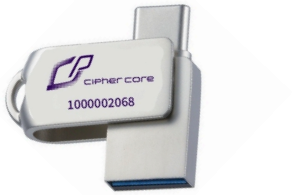
損害発生のリスク



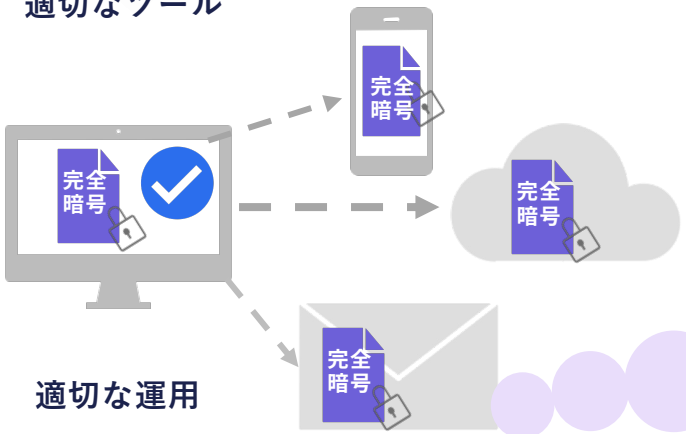
実効的な情報セキュリティ対策

暗号化など適切な**ツール利用**と簡潔な**運用ルール**を全員が実践することにより、

効率的に対応できるスキルと組織力が手に入ります



適切なツール



適切な運用

業務効率化

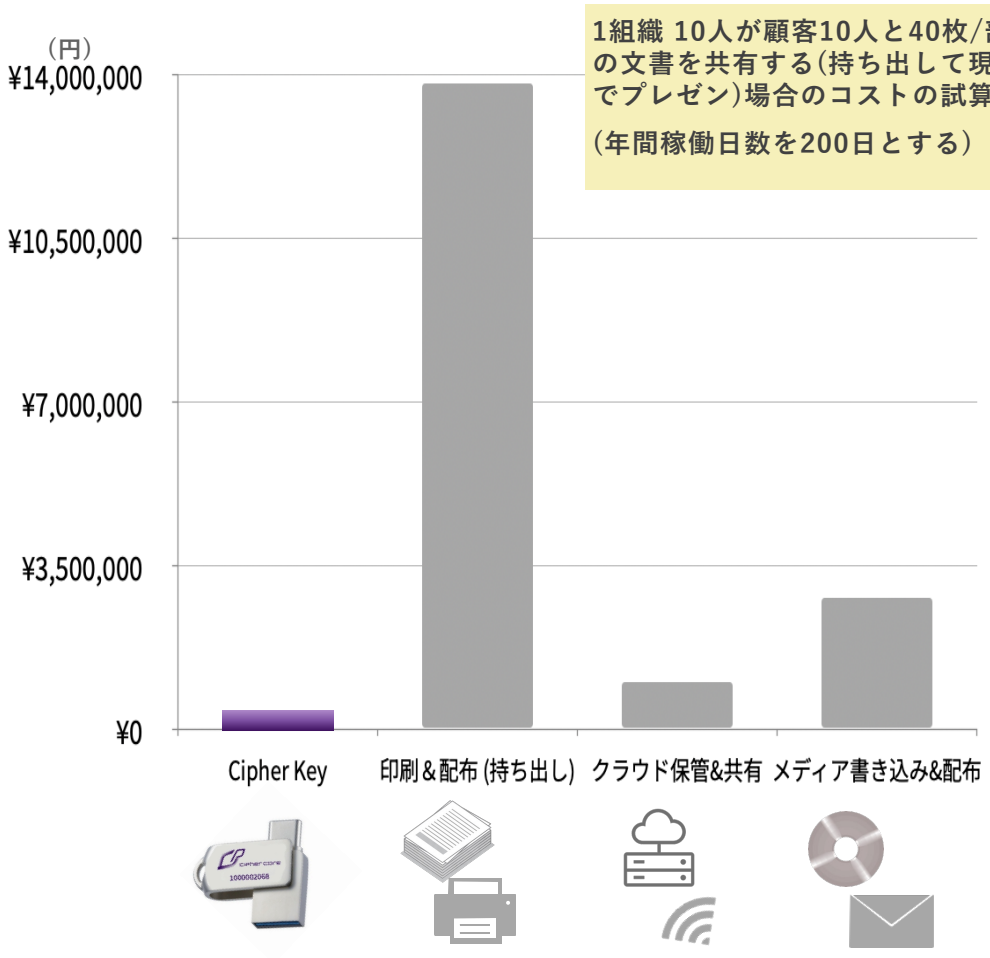
情報共有コストの低減

生産性の向上

完全暗号化した情報は、漏洩してもただのゴミに過ぎない

Cipher Keyを用いる情報共有コストの低減 (1)

情報を安全に持ち出して共有する場合のコスト比較



1組織 10人が顧客10人と40枚/部の文書を共有する(持ち出して現場でプレゼン)場合のコストの試算

(年間稼働日数を200日とする)

Cipher Keyを用いるコスト削減効果

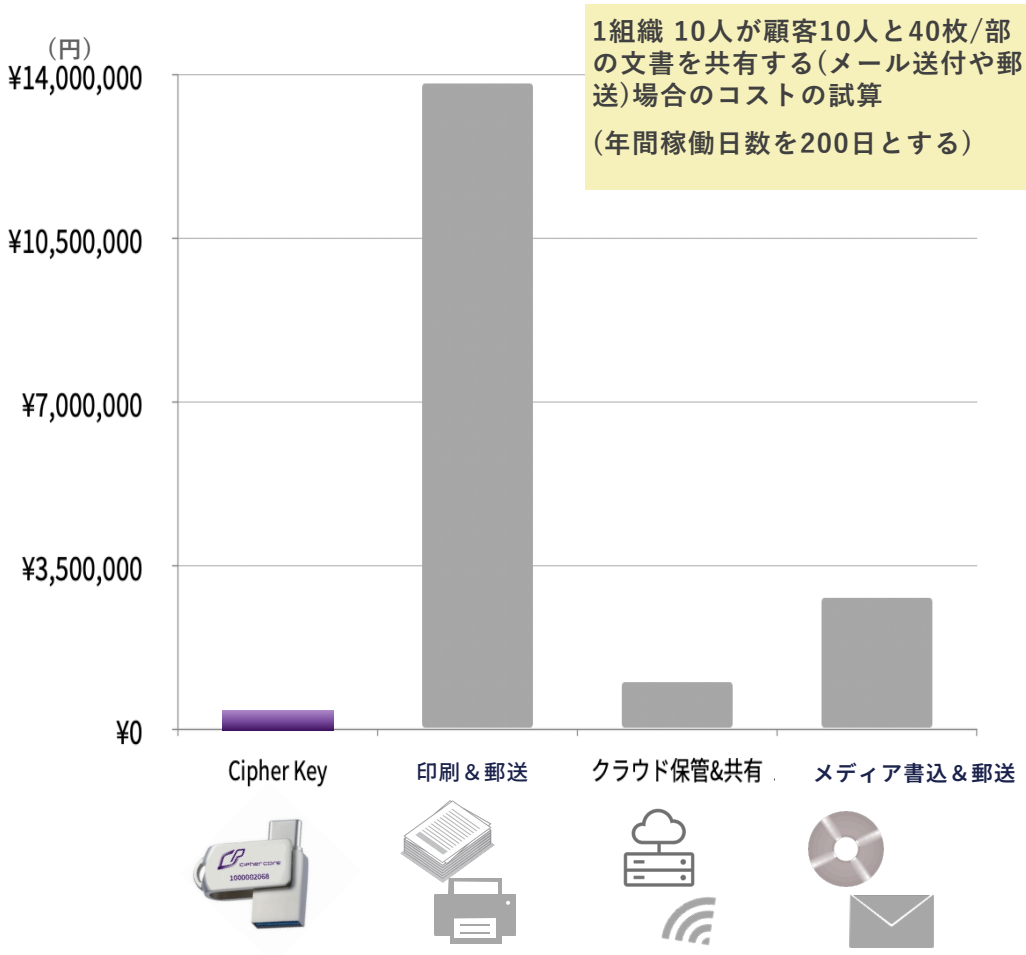
削減率
- **97%** (印刷＆配布に比べて)
- **60%** (クラウド保管＆共有に比べて)
- **85%** (書込＆配布に比べて)

暗号化を含めたトータルコストの低減はもちろん、物理的紛失を回避し、中間者攻撃・ハーベスト攻撃に晒されることなく最も安全に共有できる。

#1：人件費は、印刷10分、書込作業30分、暗号化やクラウド作業5分 時給は1,800円で計算
#2：Cipher Keyは、買い切り 350USD /人、耐用年数5年で計算
#3：クラウドストレージ利用は年額 10,000円/人で計算
#4：ファイル暗号化ソフト 年額 1,000円/人で計算
#5：VPN(社外利用も想定) 年額 60,000/人で計算
#6：用紙＆印刷費用 16.5円 /枚で計算

Cipher Keyを用いる情報共有コストの低減 (2)

情報を安全に送付して共有する場合のコスト比較



1組織 10人が顧客10人と40枚/部の文書を共有する(メール送付や郵送)場合のコストの試算

(年間稼働日数を200日とする)

Cipher Keyを用いるコスト削減効果

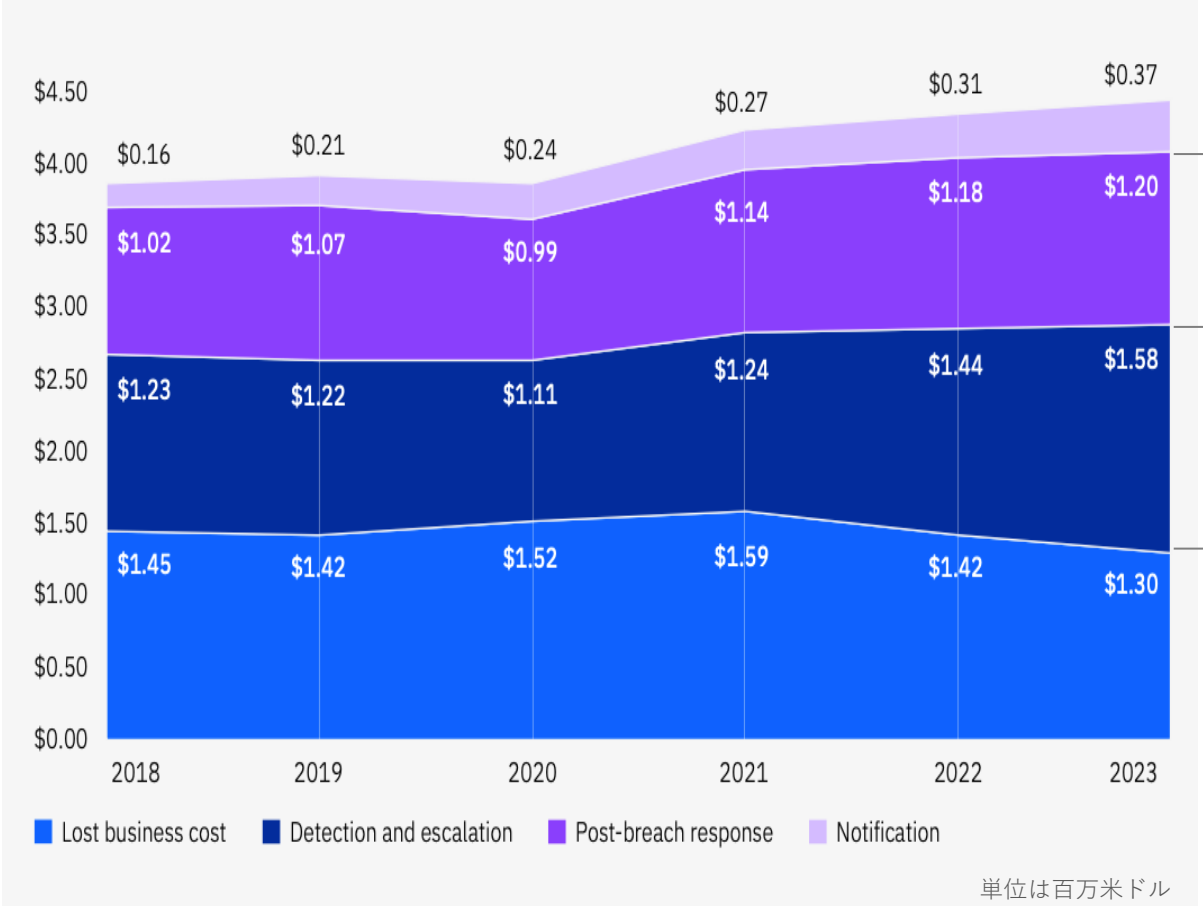
削減率
- 97.5 % (印刷＆郵送に比べて)
- 63 % (クラウド保管＆共有に比べて)
- 95.5 % (書込＆郵送に比べて)

暗号化を含めたトータルコストの低減はもちろん、物理的紛失を回避し、中間者攻撃・ハーベスト攻撃に晒されることなく最も安全に共有できる。

#1：人件費は、印刷10分、書込作業30分、暗号化やクラウド作業5分 時給は1,800円で計算
#2：Cipher Keyは、買い切り 350USD /人、耐用年数5年で計算
#3：メールやクラウドストレージ利用は年額 10,000円/人で計算
#4：ファイル暗号化ソフト 年額 1,000円/人で計算
#5：VPN(社外利用も想定) 年額 60,000/人で計算
#6：用紙&印刷費用 16.5円/枚、郵送はレターパック520円/部で計算

データ侵害の経済コストは莫大

データ侵害を受けると発生するコスト



通知コスト
- データ主体へのメール、手紙、外部への電話など通知対応
- 規制要件の特定
- 規制者との連絡
- 外部専門家への相談

侵害後の対応
- 外部からの連絡、クレジット・モニタリングおよびID保護サービス
- 新規アカウントまたはクレジットカードの発行
- 法的費用、規制当局により科される罰金、製品値引き

検知・エスカレーション コスト
- 犯罪調査およびその他の調査活動
- 評価および監査サービス
- 危機管理
- 役員や幹部職員への報告

機会損失コスト
- 犯罪調査およびその他の調査活動
- 評価および監査サービス
- 危機管理
- 役員や幹部職員への報告

Source：データ侵害のコストに関する調査2023年（IBM Security）https://www.ibm.com/jp-ja/reports/data-breach

Cipher Keyを用いるデータ侵害の経済コストの低減

データ侵害のコストは？

保有レコード	保有レコード数
顧客個人情報	500
従業員個人情報	30
財務情報や顧客リストなど機密・専有データ	300
知的財産情報	20
匿名化した顧客情報	100

データ侵害コストの試算

合計

¥21,804,000

保有レコード	保有レコード数	コスト
顧客個人情報	500	¥12,150,000
従業員個人情報	30	¥720,000
財務情報や顧客リストなど機密・専有データ	300	¥6,690,000
知的財産情報	20	¥414,000
匿名化した顧客情報	100	¥1,830,000

Cipher Key
ツール

0 or 低減

※試算コスト詳細（1レコードあたり）
顧客の個人情報　24,000円
従業員の個人情報　24,000円
財務情報やリスト等機密専有データ　22,300円
知財情報　20,700円
匿名化した顧客情報　18,300円

表：各レコード固有の侵害コスト金額(円換算)/件で計算 (通貨換算レート 132.75 JPY/USD)
IBM SecurityのReportを参照 (https://www.ibm.com/jp-ja/reports/data-breach)

顧客との信頼構築

顧客が最も信頼をおくのは？

顧客のデータを守る組織

消費者は、企業との信頼構築において
データ保護を最も重要視すると回答

調査対象：企業経営者500名
消費者2,508名
従業員2,012名
調査時期：2023年
国：米国

Source：PwC 2023年信頼調査
https://www.pwc.com/us/en/library/trust-in-business-survey-2023.html

人的資本可視化と情報セキュリティツール活用研修 ［決定版］

リスク回避だけでなく機会創出につながる情報セキュリティ研修＝人的資本強化施策

**情報セキュリティ
ツール活用研修
［決定版］**

1. 効率的で安全なデータ利活用
2. コンプライアンス向上
3. 従業員のスキルと士気の向上

**開示すべき
人的資本情報**

人材育成	研修時間/参加率、複数分野受講率、人材開発効果
従業員満足度	柔軟な働き方、キャリアアップ、成長
流動性	人材定着、新規雇用促進
多様性	
健康・安全	労働災害防止、ヘルスケア
労働慣行	リモートワーク推進、残業減少
コンプライアンス	規制遵守／倫理

- 企業価値向上
- ブランド価値向上
- 顧客満足度向上
- 情報漏洩コスト削減
- 収益/利益増加
- 競合との差別化
- イノベーション促進
- 新規顧客/投資家獲得

有用な人的資本強化施策として活用できるセキュリティ研修

◆ キャリア開発、DX人財育成に関する開示事例 ①・・・西日本旅客鉄道株式会社

西日本旅客鉄道株式会社(E04148)
有価証券報告書

（イ）主な施策

① 自律的なキャリア開発機会の拡充	・ポスト公募（注３）を通じた自律的なキャリア選択機会の拡充 ・Off-JTメニューや資格取得支援の拡充 ・副業の奨励やグループ外派遣を通じた幅広い社外経験の支援 ・新たな事業創出支援、事業化機会の提供 （イノベーション創出プログラム）（注４）
②（グループ経営人財候補対象） キャリアディベロップメントプログラムの導入	・複数の事業、業務経験と戦略上重要な専門性の獲得を意図したジョブローテーション ・専門性獲得に向けたビジネスリテラシーの習得支援
③（50歳以上の管理職対象） ネクストキャリアプログラムの導入	・キャリア研修を通じた保有スキルの棚卸 ・リスキリングメニューの整備やリカレント支援 ・新たなキャリアへの挑戦を含むキャリア選択機会の提供

②指標及び目標
ア．KPI（注５）
（ア）人財育成

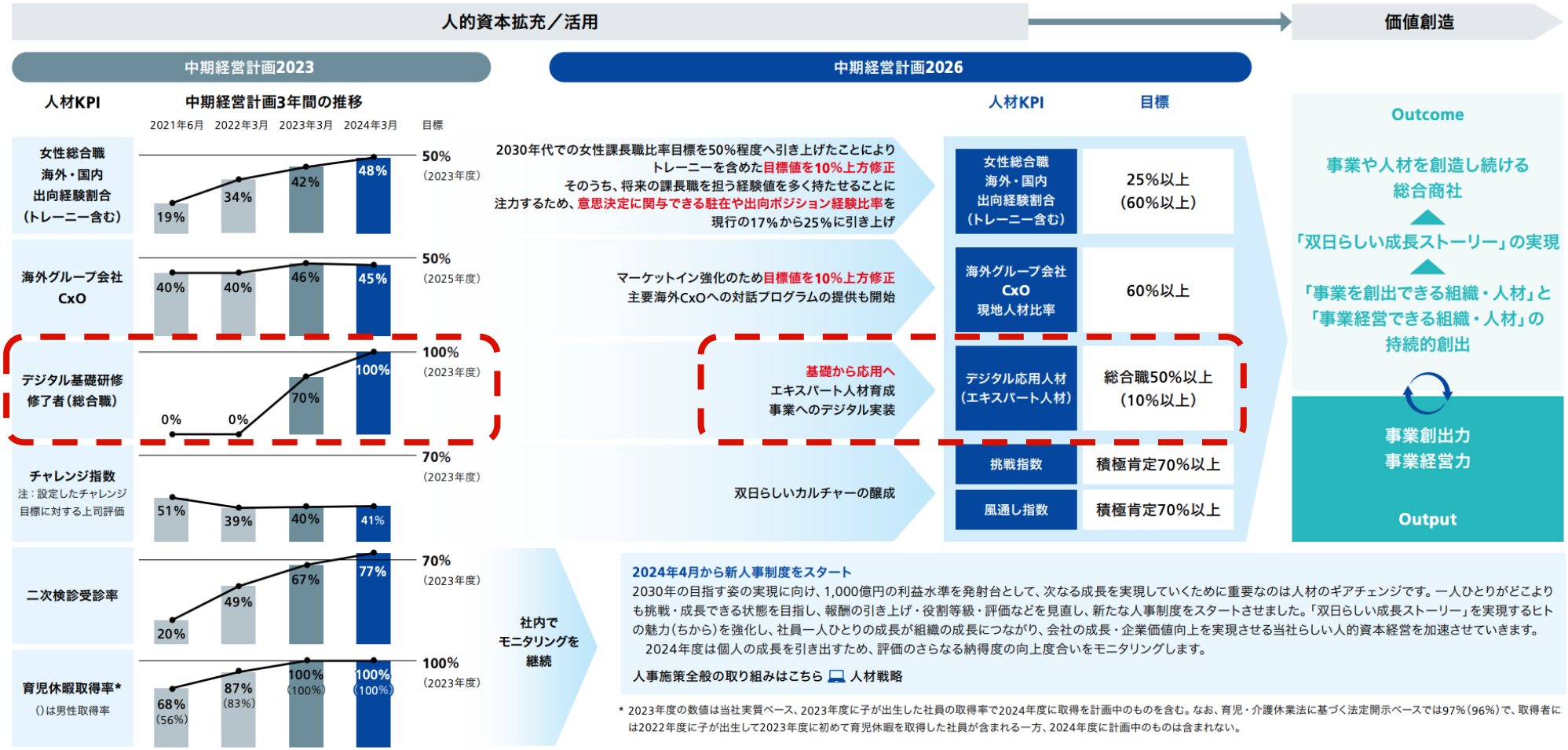
（注６）

指標	2022実績	2025目標	2027目標
（全社員） キャリア形成を支援する各種制度の利用者数	約1,000名	-	2,000名
（管理職登用候補） 複数の専門性獲得者の割合	（注７） -	-	30%
（次世代経営人財） 準備率（注８）	167%	330%	400%
上記のうち、「移動に連動しない事業」に係るスキル保有者の割合	13%	-	40%

出典：西日本旅客鉄道株式会社 有価証券報告書
（2023年6月提出）

有用な人的資本強化施策として活用できるセキュリティ研修

◆ キャリア開発、DX人財育成に関する開示事例 ② ・・・双日株式会社



2024年4月から新人事制度をスタート

2030年の目指す姿の実現に向け、1,000億円の利益水準を発射台として、次なる成長を実現していくために重要なのは人材のギアチェンジです。一人ひとりがどこよりも挑戦・成長できる状態を目指し、報酬の引き上げ・役割等級・評価などを見直し、新たな人事制度をスタートさせました。「双日らしい成長ストーリー」を実現するヒトの魅力（ちから）を強化し、社員一人ひとりの成長が組織の成長につながり、会社の成長・企業価値向上を実現させる当社らしい人的資本経営を加速させていきます。

2024年度は個人の成長を引き出すため、評価のさらなる納得度の向上度合いをモニタリングします。

人事施策全般の取り組みはこちら 人材戦略

* 2023年度の数値は当社実質ベース、2023年度に子が出生した社員の取得率で2024年度に取得を計画中のものを含む。なお、育児・介護休業法に基づく法定開示ベースでは97%（96%）で、取得者には2022年度に子が出生して2023年度に初めて育児休暇を取得した社員が含まれる一方、2024年度に計画中のものは含まれない。

出典：双日株式会社 統合報告書2024

人的資本の可視化と資金調達

「人的資本の可視化」はすでに始まっている

企業の人的資本経営における取組をスコアリングし、一定以上スコア取得事業者へ融資等

日本経済新聞

朝刊・夕刊　LIVE　Myニュース　日経会社情報　人事ウオッチ　NIKKEI Prime

トップ　速報　ビジネス　マーケット　経済　国際　オピニオン　もっと見る

人的資本経営、大手銀行が開示支援　アプリで研修把握

金融機関　＋フォローする

2024年4月22日 5:00 [会員限定記事]

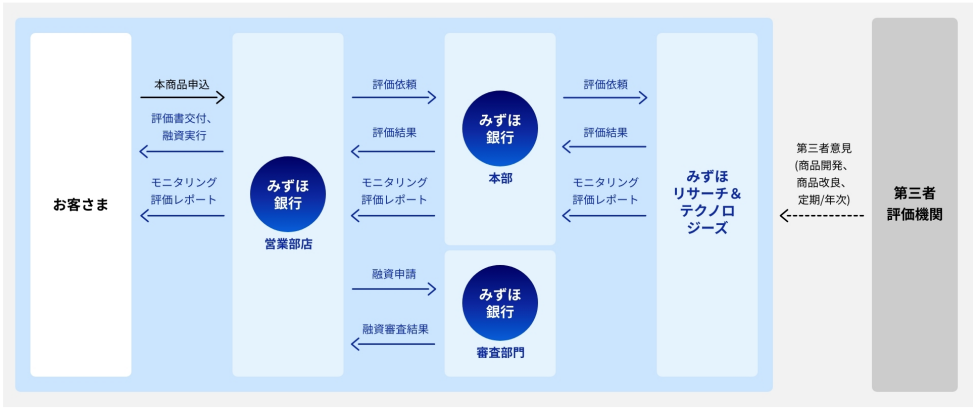
保存

企業が進める人的資本経営の情報開示を巡り、大手銀行がシステムの提供を通じた支援に乗り出す。三菱UFJ信託銀行は年度内にも従業員の研修状況などを企業が把握できるアプリを開発し、記載につなげる。三井住友銀行も支援システムを無償提供する。開示のインフラ整備に悩む企業が増えており、取引拡大の契機にする。

アプリを使って研修の状況を把握しやすく

政府は2023年、大手企業を対象に有価証券報告書で人的資本...

（例）みずほ銀行



「Mizuho人的資本経営インパクトファイナンス」のスキーム図

当研修が解決する課題

効果的な対策として何をすれば良いかわからない
重大な情報漏えいが発生しないか、不安だ
対策と教育のための人材が不足・手がまわらない

解決

実効的な対策スキルの習得

情報セキュリティの本質を正しく理解した上で、完全暗号による暗号化など有用なツールを導入し、ツールを適切な組合せで適切に使用することで、脅威に対応可能なスキルを身につけることができます。

不正の抑止及び堅牢な情報保護

情報セキュリティツール利用の技能訓練と併せて秘密情報取扱いに関する法律を学ぶことで、不正が抑止され、秘密情報が適切に管理されるビジネス環境が手に入ります。

効率的かつ経済的な学習管理

eラーニングによる教育プログラムを提供することで、従業員の個別化したスケジュールに対応できます。
LMS(Learning Management System)による進捗管理と修了証書発行を図れるため、人材開発部門の負担を軽減できます。

研修サービス内容 (1)

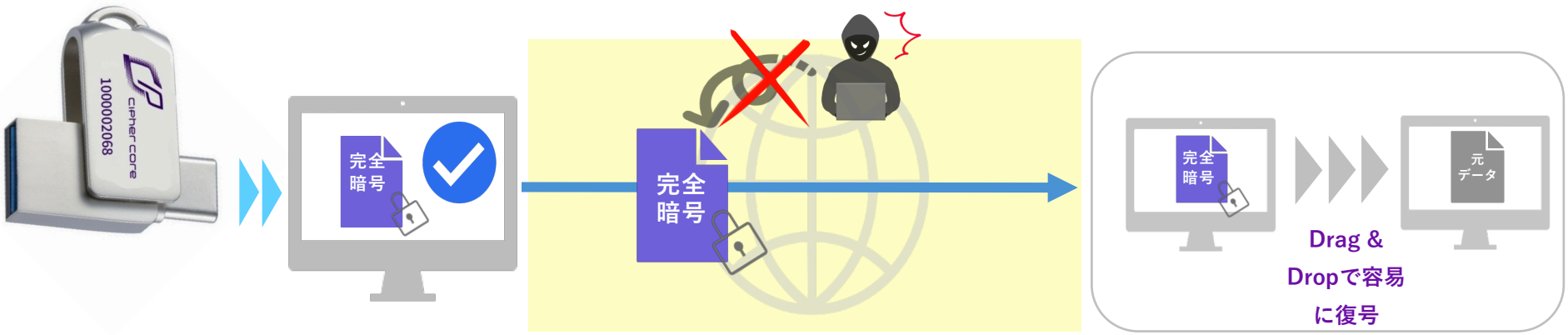
オンラインで受講できる人材開発訓練を提供

効果的な情報セキュリティ対策のための、ツールを導入・利用する技能習得と情報漏洩対策実施に有用な、中小企業から大企業まであらゆる組織向けの従業員教育サービスです。

機能・サービス内容	詳細
情報セキュリティツール活用研修［決定版］	情報を強固に守る情報セキュリティツールの導入・利用における技能訓練と併せて、不正競争防止対策、個人情報保護対策および秘密情報管理を全関係者に周知徹底し、日々の業務を適切に遂行するための従業員教育を提供します。 これにより、情報セキュリティの本質を正しく理解し、ツールを適切な組合せで適切に利用して、情報セキュリティ上の脅威に対して対応可能なスキルを身につけることができます。

研修サービス内容 (2)

完全暗号(※)化ができるツールを導入



※ 完全暗号：どんな方法を使っても永久に破ることができないことが証明されている暗号技術

高度な暗号化がされた個人情報は、盗まれても情報漏洩にはなりません

『個人情報保護委員会ガイドライン』

「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ

（令和５年 12 月 25 日更新）

・漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、**「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合については、報告を要しない**

・「高度な暗号化等の秘匿化がされている場合」とは、第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要

教育プログラム 内容

1	イントロダクション	1. なぜ情報セキュリティツールを使用して情報を守らなければならないのか	2. 本研修の構成と流れ
2	情報セキュリティ対策の基本とツールの使い方 (情報セキュリティ対策の基本に沿ったツールの使い方について学びます)	1. 情報セキュリティインシデントの実例紹介	3. 情報セキュリティ対策の基本と具体的対策
		2. 情報セキュリティインシデントの分類	4. 情報セキュリティインシデントに対するツールを使った具体的対策
3	情報セキュリティツールの導入 (一般的な情報セキュリティツールについて学びます)	1. 暗号化ツール	4. VPN ツール
		2. バックアップツール	5. ツール使用についてのまとめ
		3.マルウェア対策ツール	
4	近未来の情報セキュリティ脅威 (近未来の情報セキュリティに関する脅威と、その対策ツールについて学びます。)	1. 量子コンピュータの時代	4. 完全暗号を用いたセキュリティツール
		2. 人工知能の時代	5. 完全暗号に基づく暗号化ツール
		3. 完全暗号による情報セキュリティ	6. Cipher Key による具体的な情報セキュリティ対策
5	法律上保護すべき情報	1. 個人情報保護法	2. 不正競争防止法

組織・企業の持続可能な成長に不可欠な、法律遵守に関する教育

当研修で実施する、不正競争防止法および個人情報保護法に則った教育は、組織・企業経営において以下の効果をもたらします。

	不正競争防止法	個人情報保護法
情報の保護	知的財産権や営業秘密の重要性を教えることで、**独自のアイデアや製品、ブランドなどを保護し、競争優位を維持**します。	個人情報保護に関する適切な手順やポリシーの確立により、**社内プロセスが効率化されデータ漏洩のリスクが低減**します。
信頼の醸成	法律遵守の姿勢を示すことで、**信頼性と評判が向上**し、他の法律遵守企業とのビジネス機会が増える可能性があります。	顧客や従業員の個人情報を適切に管理することで信頼を得られ、**長期的な関係を築き、市場での競争力が向上**します。
不正の抑止	従業員の意識が高まり、不正行為を防ぐ文化が醸成されます。	法律に関する教育を通じて、個人情報を取り扱う際の意識が高まり、不注意によるミスの発生や不正を抑制できます。
法的リスクの低減	**経営者は秘密情報管理教育の責務を履行**することで、従業員は法を理解し遵守することで、**法的トラブルにおけるリスクを低減**できます。	法律遵守により、**罰金や訴訟などのリスクを回避**できます。

料金　（中小企業の場合）

人材開発支援助成金を活用できる職業訓練（#1）です。

４０万円 / 従業員（税込）

オンライン教育（標準学習時間：15時間）

上記 **経費の75%（上限30万円）の助成**が受けられます。（#2）

（#1）雇用保険適用事業所の事業主への「事業展開等リスキリング支援コース」の対象となります。
　　デジタル技術を活用して業務効率化を図ったり顧客サービスを提供する等、あらゆる企業が対象となります。
（#2）中小企業の助成額です。大企業の場合は、60%の経費助成で上限は20万円です。
（#3）申請における書類の作成や申請対応等もサポートしますのでご安心ください。

料金（大企業[＊]の場合）

人材開発支援助成金を活用できる職業訓練（#1）です。

４０万円 / 従業員（税込）

オンライン教育（標準学習時間：15時間）

上記 経費の60%（上限20万円）の助成が受けられます。（#2）

[＊] 次頁で説明する「中小企業」以外の企業を説明上「大企業」と書いています。
(#1) 雇用保険適用事業所の事業主への「事業展開等リスキリング支援コース」の対象となります。
　　デジタル技術を活用して業務効率化を図ったり顧客サービスを提供する等、あらゆる企業が対象となります。
(#2) 中小企業以外の助成額です。中小企業の場合は、75%の経費助成で上限は30万円です。
(#3) 申請における書類の作成や申請対応等もサポートしますのでご安心ください。

中小企業事業主の範囲について

「主たる事業」ごとに**A,Bどちらかの基準に該当**すれば、中小企業事業主となります。

主たる事業	A.資本金の額または出資の総額	B.企業全体で常時雇用する労働者の数
小売業(飲食店を含む)	5,000万円以下	50人以下
サービス業	5,000万円以下	100人以下
卸売業	1億円以下	100人以下
その他の業種	3億円以下	300人以下

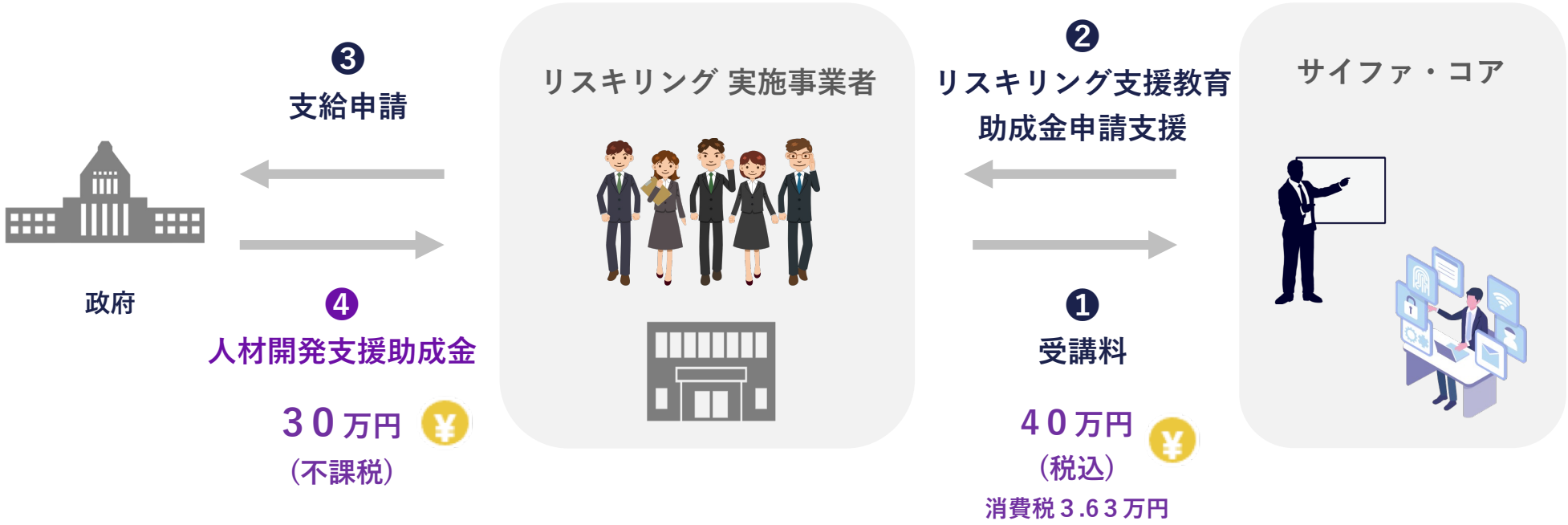
※1.個人事業主で従業員を雇っている場合でも、雇用保険に加入していれば対象となります。
(雇用保険加入者数の条件が中小企業の規模に該当する場合に限ります)

※2.資本金等を持たない事業主は「B企業全体で常時雇用する労働者の数」によって判断します。

※3.「主たる事業」は、総務省の日本標準産業分類の「業種区分」に基づきます。
https://www.soumu.go.jp/toukei_toukatsu/index/seido/sangyo/R05index.htm

サービスと助成金の流れ（1）-a（中小企業の場合）

中小企業の事業者が、雇用保険被保険者である従業員１人に対して、eラーニングによる事業外訓練（#1）を実施した場合

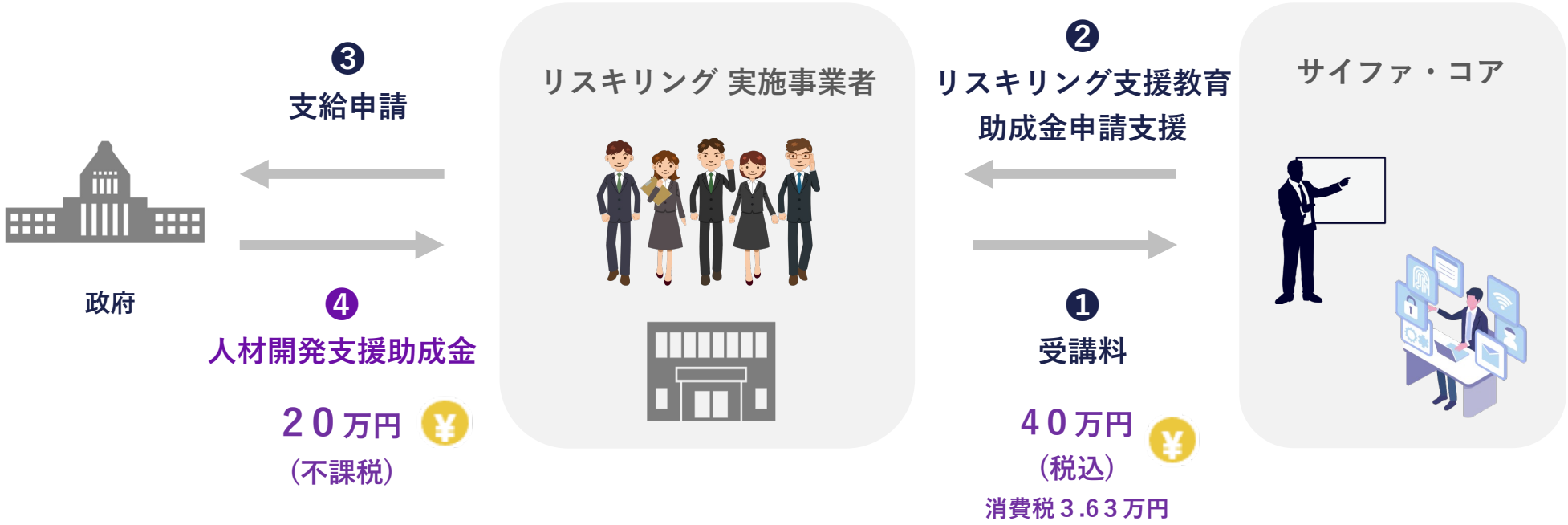


（＃１：事業展開等リスキリング支援 OFF－JTとして実施されるeラーニングによる事業外訓練）

サービスと助成金の流れ (1) -b (大企業 [＊] の場合)

（＊P7で説明する「中小企業」以外の企業を説明上「大企業」と書いています。）

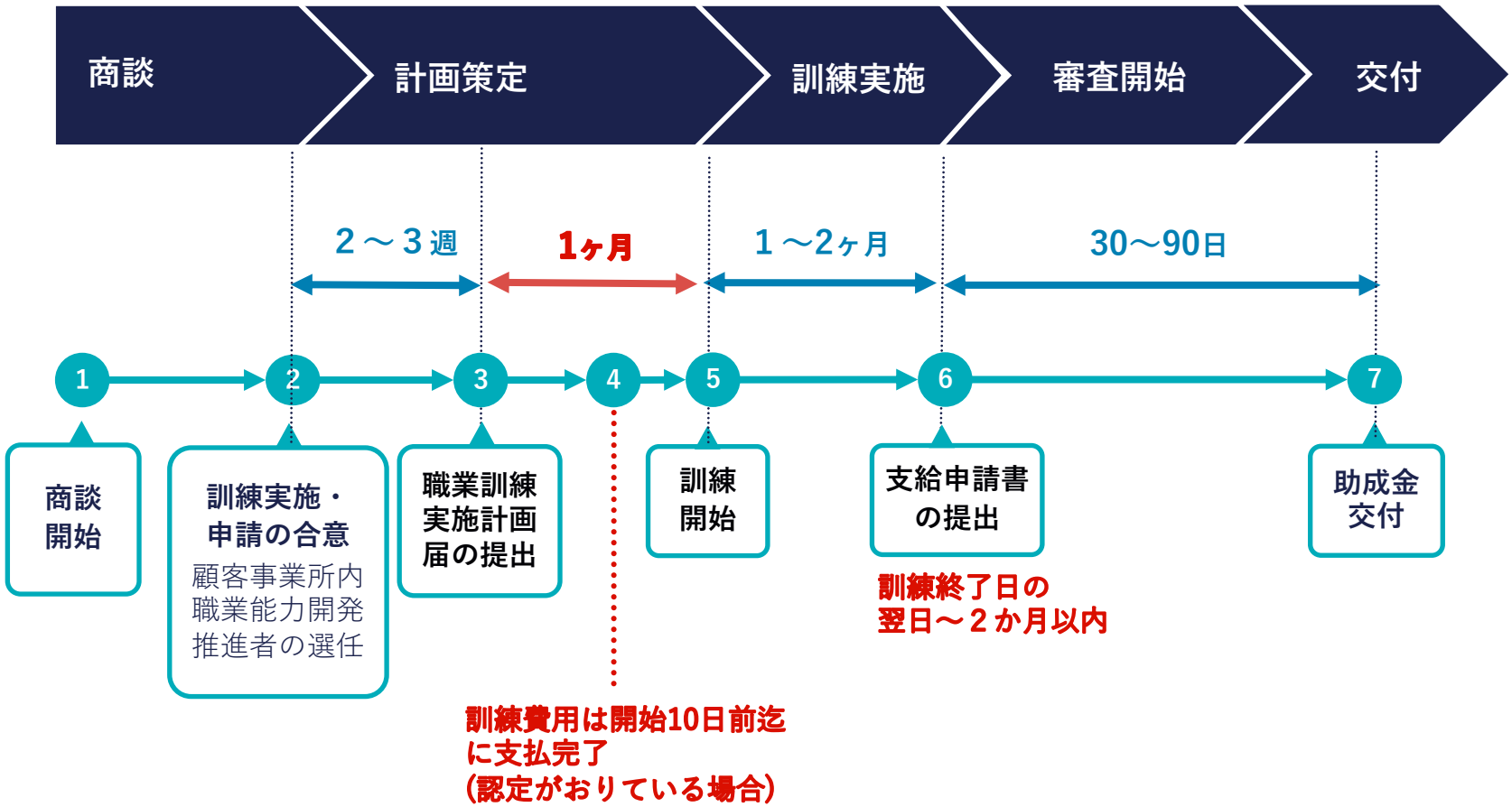
大企業の事業者が、雇用保険被保険者である従業員１人に対して、eラーニングによる事業外訓練 (#1) を実施した場合



（＃１：事業展開等リスキリング支援 OFF－JTとして実施されるeラーニングによる事業外訓練）

営業および教育訓練実施プロセス

営業および教育訓練実施プロセスを、以下のとおり想定しています。



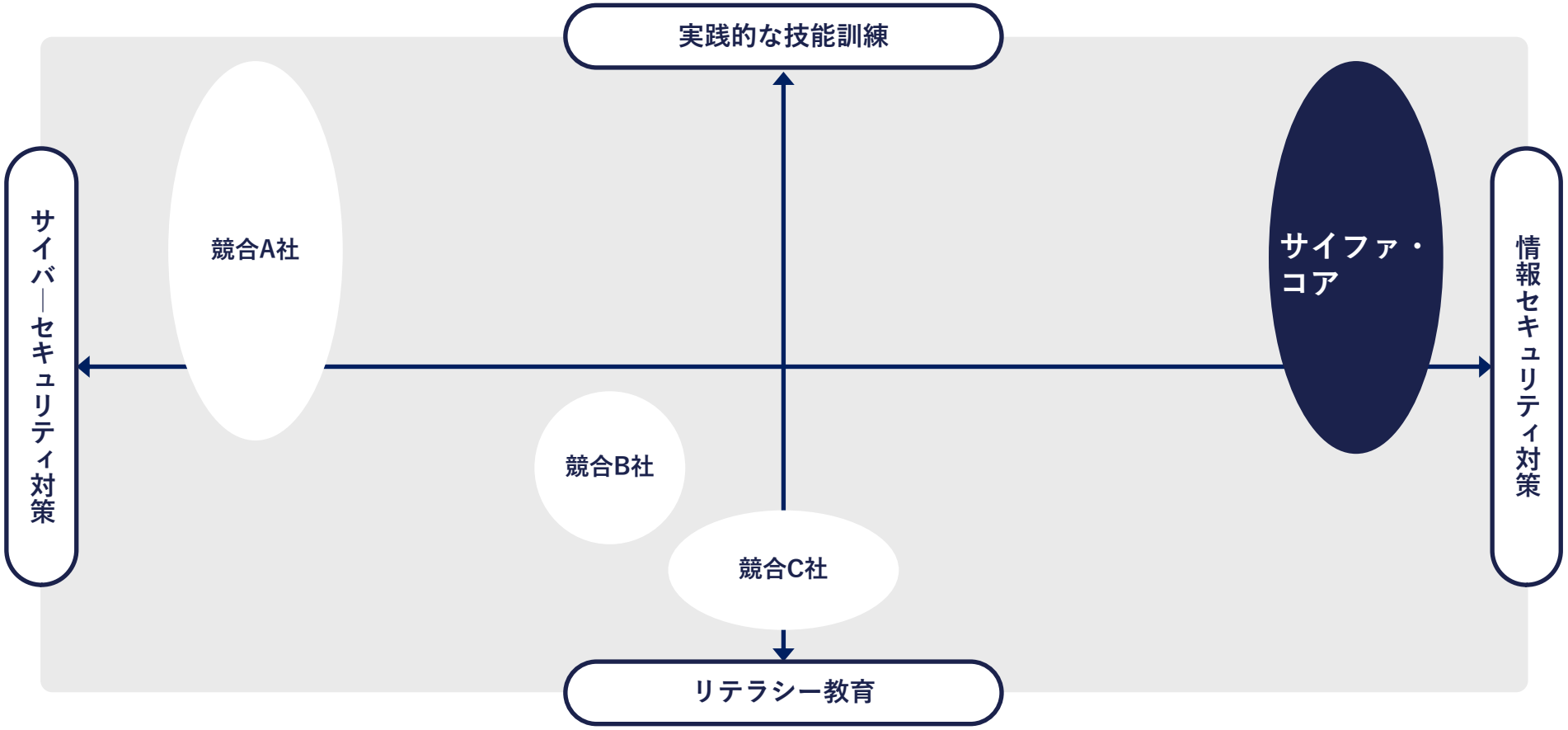
お客様

情報セキュリティツール活用研修［決定版］がお役に立てるお客様は以下のとおりです。

	助成金支給を受ける場合	助成金支給を受けない場合
事業主	• 雇用保険適用事業所の事業主である • 事業内職業能力開発計画及びこれに基づく職業訓練実施計画届を作成し労働者に周知している • 従業員に対して賃金を適正に支払っている • 審査必要書類を整備、５年間保存している	• 左記の要件を満たさない事業主
従業員	• 雇用保険法第４条に規定する被保険者 • 計画届時に提出した対象者である被保険者 • 訓練受講時間数が、実訓練時間数の８割以上 • 訓練等の受講を修了	• 左記の要件を満たさない従業員
業界・業種	• 全業種	• 全業種
部署・部門	• 全部署、全部門	• 全部署、全部門
その他	• デジタル技術を活用して業務の効率化を図る組織 • デジタル技術を活用して製品やサービス、ビジネスモデルを変革する組織 • コンプライアンス要件のある組織 • システムアップグレード計画のある組織 など	―――

他社との違い(1)

当社は他社と比較して、情報セキュリティツールを使用する技能訓練及び最新の対策の教育に加えて、完全暗号を適用する高度な情報セキュリティツールを提供できる点が強みであり、「現場で活かせる実践的な情報セキュリティ技能の習得」「強固な情報セキュリティ対策」を重視する企業様に選ばれています。



他社との違い (2)

A社: サイバー攻撃の被害を想定した演習、B社: セキュリティ対策のeラーニング研修と比較して、認知度や導入実績の点が劣るものの、「高度な情報セキュリティツールの活用訓練」 「最新かつ近未来の脅威に対応できる情報セキュリティ対策」「法律遵守に関する教育」に特化している点が当社の強みです。

	当社		競合A社		競合B社	
実践的な技能訓練(演習)	◎	情報セキュリティの専門家が、情報セキュリティツールを使用する技能訓練と情報漏洩対策を教育	◎	サイバー攻撃やマルウェアの仕組み、リスク管理、インシデント対応等、体験型演習にて学習	△	情報セキュリティの脅威と対策、標的型攻撃メール対策のほか、ウイルス感染デモを体験学習
最新の情報セキュリティ対策に関する教育	◎	近未来の情報セキュリティに関する脅威と、その対策ツールについても教育	×	サイバーセキュリティの動向や最近の事故事例の紹介(情報セキュリティ教育は軽微)	△	昨今の脅威の動向やIPA情報セキュリティの10大脅威等を学習
情報セキュリティツール導入	◎	世界唯一無二の高度な暗号技術製品をはじめとするツール導入支援	×	―	×	―
認知度	×	企業・サービス名の認知度は低度	◎	取引先は伊藤忠テクノソリューションズ、文部科学省、農林水産省等	○	導入実績は累計2万人以上
料金	△	40万円／人 ／回 (≒11時間) (実質負担額は10～20万円)＊参考	△	75,000円／人 ／回 (7～8時間)	○	19,800円／人 ／回 (7～8時間)
助成金の適用 (＊)	◎	人材開発支援助成金を活用可能 (中小企業75%(上限30万円)、 大企業は60%(上限20万円) 助成	×	―	×	―
不正競争防止法と個人情報保護法	◎	法律遵守に関する教育を併せて実施し、企業・組織の成長に貢献	×	―	×	―

会社概要

コア技術： 完全暗号 “COMPLETE CIPHER” （情報理論的安全性に基づく）

会社名	サイファ・コア株式会社
CEO	中村 宇利
会社所在地	東京都港区港南1丁目9番36号 アレア品川13階
URL	https://www.cipher-core.com/
MAIL	info@cipher-core.com
資本金	１億円（資本準備金含む）
設立年	2021年

情報セキュリティツール活用研修

［決定版］

サイファ・コア株式会社