Crossing makes the Future.

船橋市　ITシリーズセミナー(第９回)

DXが進むと益々重要になる デジタルセキュリティ

2024/11/27

NTTテクノクロス株式会社

セキュアシステム事業部

NTTテクノクロス

講師プロフィール：田村　基樹

経歴

- ２００６年NTTソフトウェア株式会社へ入社
- 通信、建設等の業界向けの営業としてシステム開発やサポートサービスを提案
- ２０１７年NTTソフトウェア社とNTTアイティ社が合併してNTTテクノクロス社が設立
- 同時期にセキュリティ分野専門の営業担当として活動を開始
- 現在は顧客のセキュリティ課題を聴取して、その対策のサービスやソリューション提案を担当、企業のセキュリティレベルの向上を進める
- その他、国際イベント等のセキュリティ対策への支援に向けた高度専門人材、セキュリティチームの派遣等も進める

アジェンダ

◆会社紹介

◆サイバー攻撃のトレンド

◆中小企業でもサイバー攻撃を受ける？

◆サイバー攻撃されたらどうなる？

◆中小企業のセキュリティ対策はどうしたら良いか？

◆情報セキュリティ5か条への対応方法

会社紹介

会社概要

商号	ＮＴＴテクノクロス株式会社 NTT TechnoCross Corporation
設立	1985年7月2日（ＮＴＴソフトウェア） 1987年6月3日（ＮＴＴアイティ） 2017年4月1日（ＮＴＴテクノクロス）
資本金	5億円
売上高	522億円（2023年度末）
社員数	1,877名(2024年3月末現在)
業務内容	1. 情報通信ネットワークを利用する情報提供、情報処理、決済(代理徴収を含む)など各種サービスの提供、各種情報制作およびそれらサービス提供に必要なシステムの賃貸・販売に関すること。 2. 情報通信システムの設計、開発、建設、販売、賃貸、管理、運用・保守およびシステム評価に関すること。 3. ソフトウェアの設計、開発、販売、賃貸、運用・保守および品質管理に関すること。 4. ハードウェアの開発、製造、販売、賃貸、設置、および保守に関すること。 5. 前各号に係わる新技術の調査、その応用開発、コンサルティング、教育および研修に関すること。 6. 前各号に係わる労働者派遣事業。 7. その他前各号に関連する一切の業務。
株主	日本電信電話株式会社

数字でわかるNTTテクノクロス

お客様と未来を共創し続ける
ソフトウェアリーディングカンパニー

NTTテクノクロス

設立

39年

1985年7月2日設立
資本金5億円

売上高

522億円

一般市場47%
2023年度末

拠点数

5拠点

田町、横浜、武蔵野、
名古屋、大阪

社員数

1,877名

技術系職　1472名　2023年度末

主要技術分野

5分野

AI、メディア、セキュリティ、
クラウド、ネットワーク

国内シェアNo.1

3製品

メール誤送信防止、特権ID管理、
リモートアクセス

資格保有者数(ハイレベル&ミドルレベル)

延べ2,553名

AWS、Azure、CISSP、等々
2024.5

企業に求められるセキュリティ対応

企業の活動における**セキュリティ対策**は、DXの推進における様々な脅威に対して必要不可欠なものである一方、その**対応は複雑多岐**に亘ります。

そのような**課題に対する適切なアドバイス、サポートを提供できるよう、エキスパート人材を日々育成**しております。

エキスパート人材による課題への適切なアドバイス

戦略マネージメント層

- セキュリティ監査
- システム監査
- インシデント ハンドリング
- ポリシー ガイドライン策定
- 個人情報保護法 対策
- リスクアセスメント
- セキュリティ教育

実務者・技術者層

- 監視・検知・対応
- 脆弱性診断・対応
- セキュアシステム 設計・開発
- セキュリティ ツール運用
- インシデント レスポンス
- マルウェア解析
- ログ監視
- 脅威情報の 収集分析

本セミナー資料の監修

（インシデントレスポンス/脅威情報収集分析）

武井 滋紀

資格等

- NTTセキュリティ認定上級(セキュリティプリンシパル)
- 情報処理安全確保支援士(009938)
- ISC2 CISSP,CCSP
- ISACA CISA
- 日本セキュリティオペレーション事業者協議会(ISOG-J) 副代表、WG6リーダー
- InternetWeekプログラム委員(2017-2024)

（個人情報保護法対策）

土屋 直子

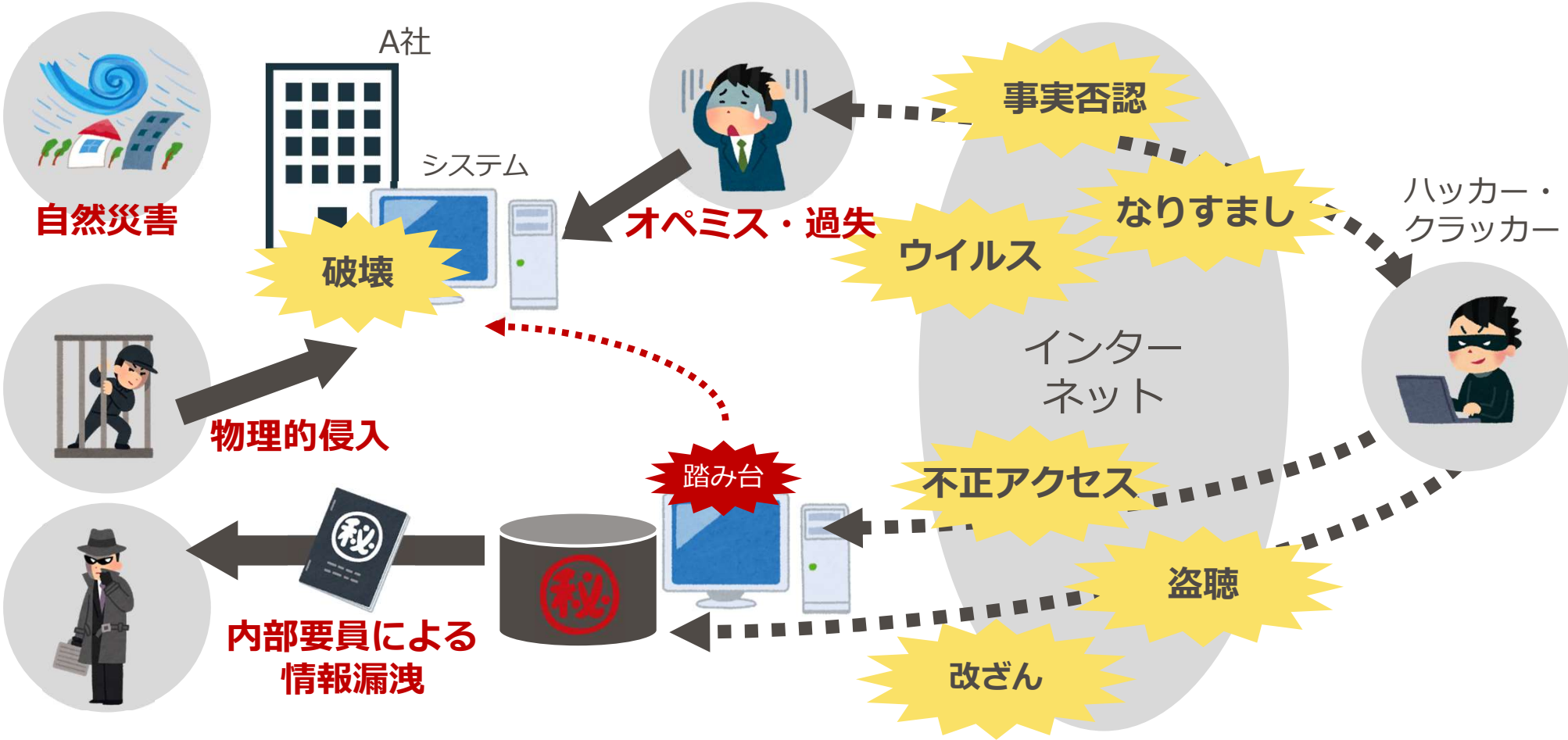
資格等

・ISMS(ISO/IEC27001)審査員
・ISO/IEC27017審査員
・ISO14001審査員補
・ISO9001審査員補
・公認情報セキュリティ監査人
・情報セキュリティアドミニストレータ
・情報セキュリティスペシャリスト
・情報処理安全確保支援士
・ISO/IEC JTC1 SC27 WG1国内委員会委員
・クラウドセキュリティ規格JIS化委員会委員
・情報セキュリティマネジメントシステムJIS原案作成委員会委員

サイバー攻撃のトレンド

企業における脅威

- 企業は様々な脅威にさらされています

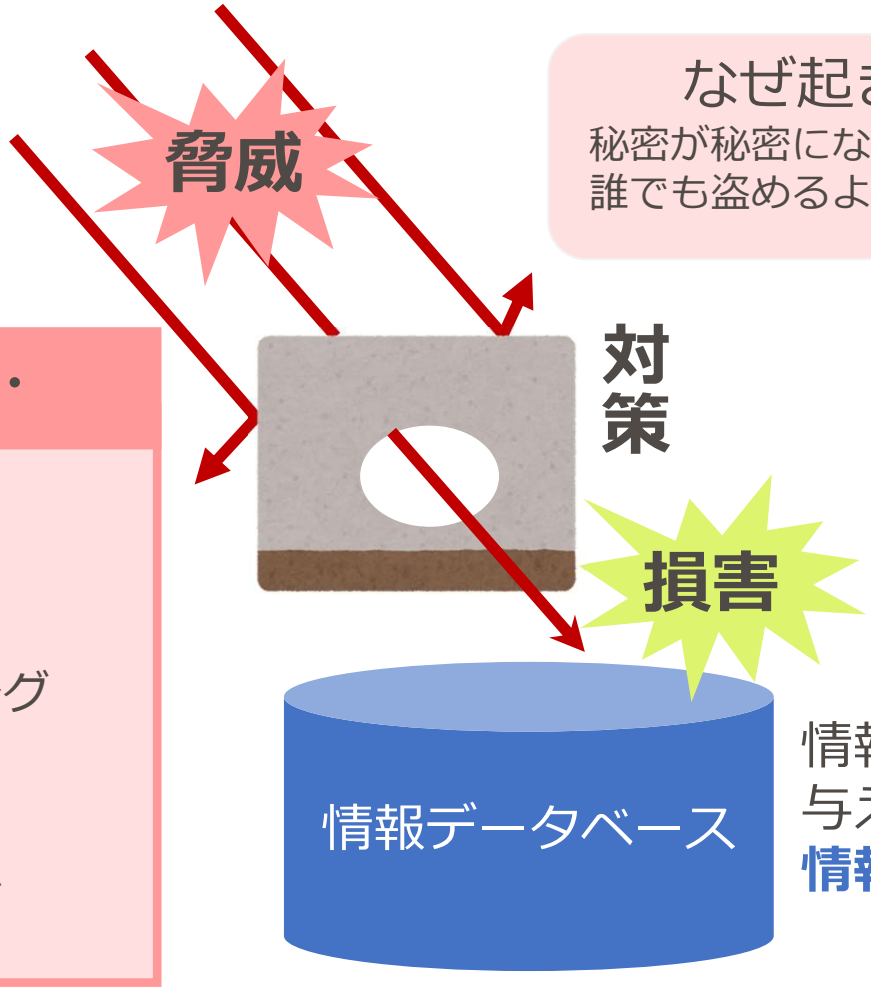


リスクは、情報システムだけとは限らない！！

情報の電子化によるメリットの反面リスクも増大！！

情報セキュリティリスクとは？

情報セキュリティリスクとは、ある脅威が、資産の脆弱性を利用して、
情報資産への損失、または損害を与える可能性のことである



脅威とは、例えば・・・

- 不正アクセス
- コンピュータウィルス
- Dos攻撃
- ソーシャルエンジニアリング
- システム障害
- 内部要因による情報漏洩
- 自然災害　　など

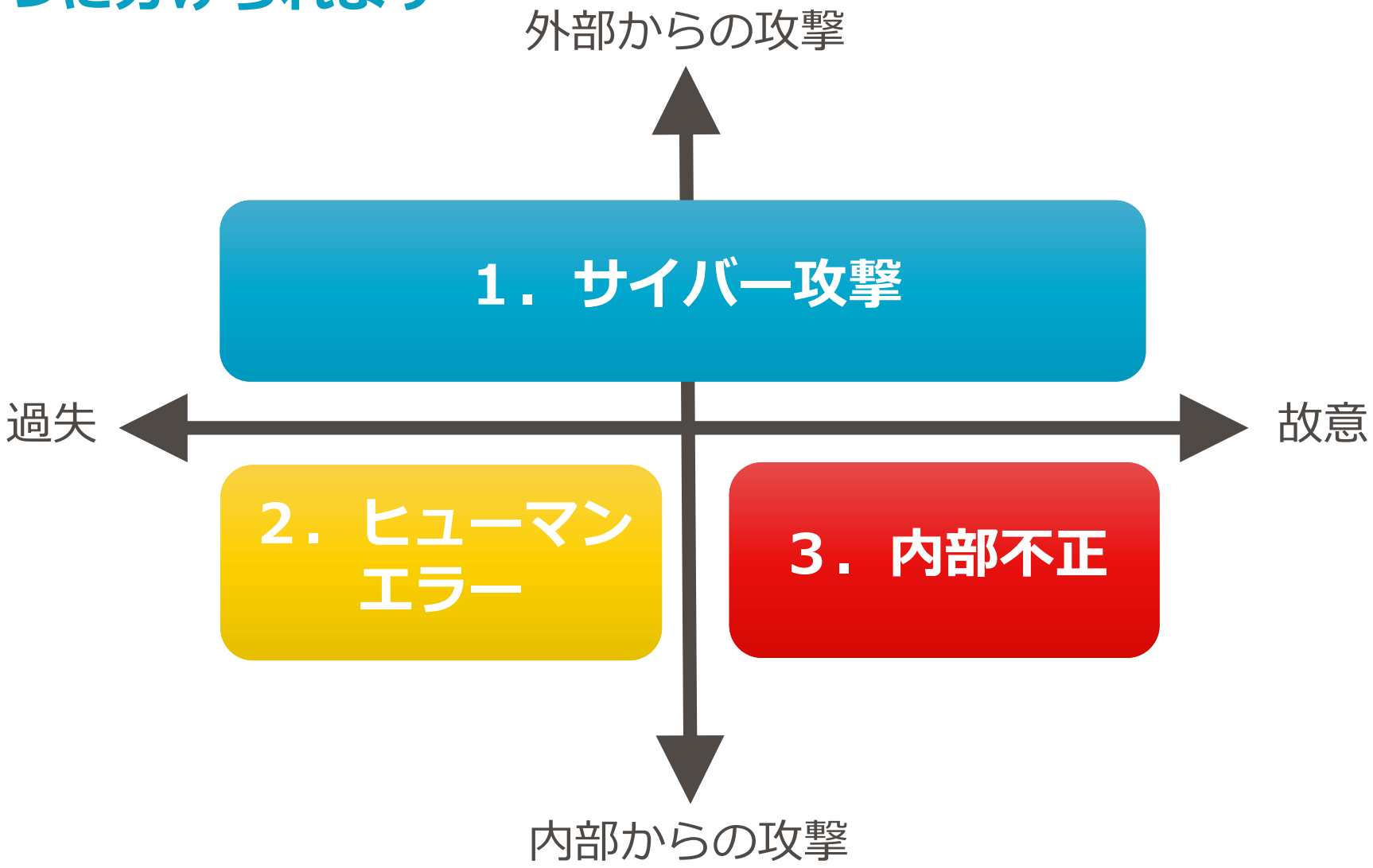
情報セキュリティの位置づけ

セキュリティはシステム関連のみと思われがちだが、ITを使う人や会社の建物、業務で扱う情報そのものまで全てに関係する

→　**これら全てがセキュリティを保って初めて成り立つ**

情報セキュリティインシデントの三大要因

- **情報セキュリティインシデントの要因を分類すると大きく3つに分けられます**



情報セキュリティ10大脅威2024（IPA）

４年連続で「ランサムウェアによる被害」が１位。
近年のランサムウェア攻撃は、標的型攻撃と同様の手法で企業・組織のネットワークに侵入したり、データを暗号化するだけでなく窃取して公開すると脅したりして、身代金を支払わざるを得ないような状況を作り出しています。
次点に「サプライチェーンの弱点を合うようとした攻撃」、「内部不正による情報漏洩」と社内外、規模、業界を問わず様々な脅威が存在することが見て取れます。

順位	タイトル　　（ ）は昨年順位
1 (1)	**ランサムウェアによる被害**
2 (2)	**サプライチェーンの弱点を悪用した攻撃**
3 (4)	**内部不正による情報漏えい等の被害**
4 (3)	標的型攻撃による機密情報の窃取
5 (6)	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6 (9)	不注意による情報漏えい等の被害
7 (8)	脆弱性対策の公開に伴う悪用増加
8 (7)	ビジネスメール詐欺による金銭被害
9 (5)	テレワーク等のニューノーマルな働き方を狙った攻撃
10(10)	犯罪のビジネス化（アンダーグラウンドサービス）

IPA10大脅威とは：
年内に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、情報セキュリティ分野の研究者、企業の実務担当者が選考

出典　IPA　情報セキュリティ10大脅威　　https://www.ipa.go.jp/security/10threats/10threats2023.html

【事例1】ランサムウェアによる被害

IT・製造業P社が提供する、全国のLPガス会社 約1000社が利用しているITシステムが、ランサムウェア攻撃を受け、検針などの顧客管理ができない状態に陥った。

■2023年6月

P社によると、外部のデータセンターに設置しているサーバーに不正アクセスの痕跡が見られ調査したところ、ハッカーによる攻撃を受けたことが発覚した。
手口は、LPガス会社に割り当てた複数のパスワードを盗んで侵入したものとみられ、**サーバーには脅迫文**が残されていた。
システム運用管理者が対策を開始したところ、**攻撃者が動きを変え、クラウド環境側のサーバー（OS, プログラム，ツールなど）の破壊や停止を実行**し、すべてのクラウドサービスの停止を余儀なくされることとなった。
なお、攻撃を受けたのは、プログラムなどのシステム稼働環境であったため、顧客情報のデータベースへの不正アクセスを受けることはなかった。
システム全面停止から復旧には、10日間を要した。

出典：https://www.purpose.co.jp/news/detail/273
https://www.nikkei.com/article/DGXZQOUE13BQ70T10C23A6000000/

ランサムウェアの脅威

「ランサムウェア攻撃」は年々巧妙化されています

攻撃者

組織的犯行グループ、犯罪者など

攻撃手法

メールから感染させる
ウェブサイトから感染させる
脆弱性によりネットワーク経由で感染させる
公開サーバに不正アクセスして感染させる

脅威と影響

PC やサーバーのデータを暗号化し、データを復旧することと引き換えに、金銭を要求する等の脅迫文を画面に表示するランサムウェアと呼ばれるウイルスの被害が確認されている。
暗号化前に重要情報を窃取し、金銭を支払わなければ窃取した情報を公開すると脅迫する攻撃 「二重の脅迫 （ double extortion）」も近年確認されている。
脅迫に従うことによる金銭的被害に加え、窃取された重要情報（組織の機密情報や個人情報等）の漏えいにより信用の失墜にもつながるおそれがある。
なお、金銭を支払ったとしても、データの復旧や漏えいした情報の削除が行われるとは限らない。

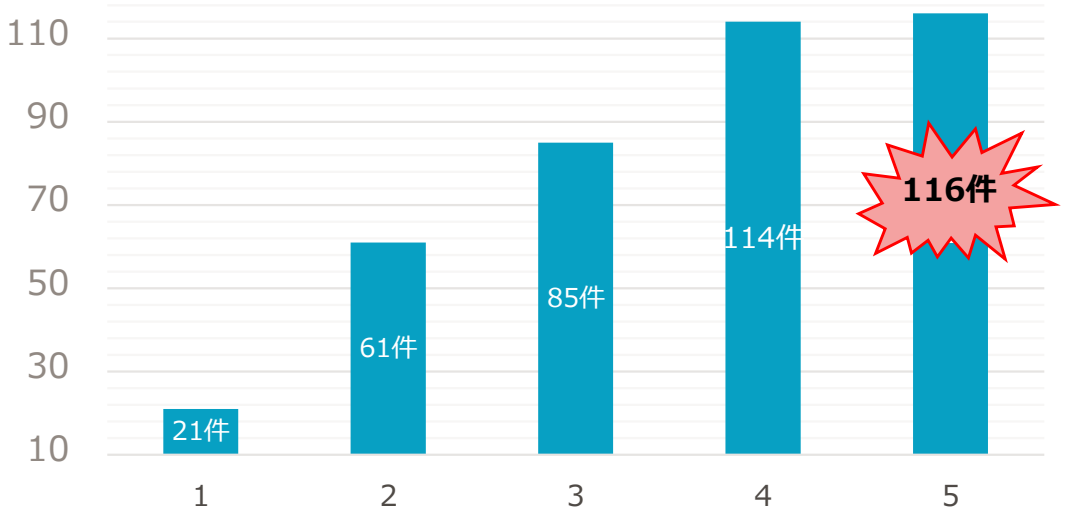
近年は、社会インフラ関連企業における被害や、病院へのランサムウェア攻撃が深刻化している。

出典：IPA【情報セキュリティ10大脅威 2023】https://www.ipa.go.jp/security/10threats/10threats2023.html

ランサムウェアの感染被害状況

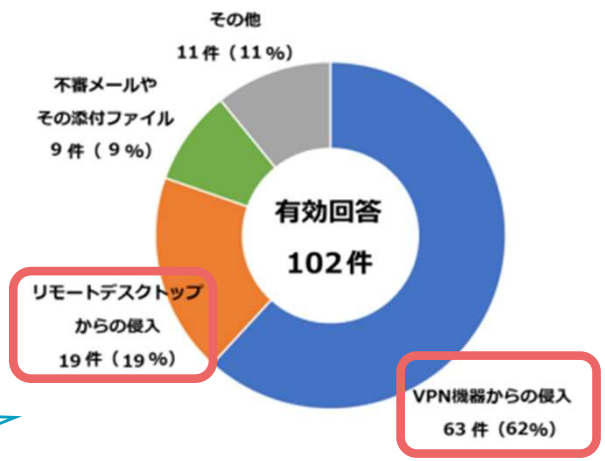
被害件数は、令和2年に比べ約5.5倍に増加している

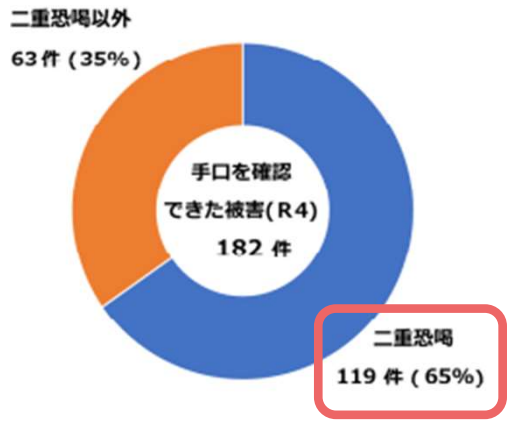
【ランサムウェアの感染被害の推移】



被害状況を件数別にみると、企業規模を問わず、犯行手口は、データの暗号化のみならず、「対価を支払わなければ当該データを公開する」などと金銭を要求する**二重恐喝が65%**であることが分かった。

感染経路は、**「リモートデスクトップ」**や**「VPN機器」**など、テレワークにも利用される機器等のぜい弱性や、強度の弱い認証情報等を利用して侵入したと考えられるものが大半を占めている。





警察庁「令和４年におけるサイバー空間をめぐる脅威の情勢等について」より

https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

ランサムウェア感染に備えた対策

様々なランサムウェア被害を防ぐための対策、及び被害を最小にするための
効果的な対策には、バックアップ取得を含めた予防の対策及び
被害を受けた後の適切な事後対応が重要です。

被害の予防

- ■インシデント対応体制の整備
- ■安易なメールの添付ファイル開封やURLクリックを行わないための教育
- ■適切なバックアップの運用
- ■共有サーバー等へのアクセス権の最小化と 管理の強化
- ■公開サーバーへの不正アクセス対策

被害を受けた後の事後対応

- ■インシデント対応手順に従った、適切なインシデント対応
- ■適切なバックアップのリストア
- ■社内外への適切な報告/連絡/相談

出典　IPA　情報セキュリティ10大脅威　　https://www.ipa.go.jp/security/10threats/10threats2023.html

【事例2】サプライチェーンの弱点を悪用した攻撃による被害

某医療センターにおいて、委託していた給食業者を発端にサイバー攻撃を受け、電子カルテ等が暗号化され、外来診療等の停止を余儀なくされる被害を受けた。

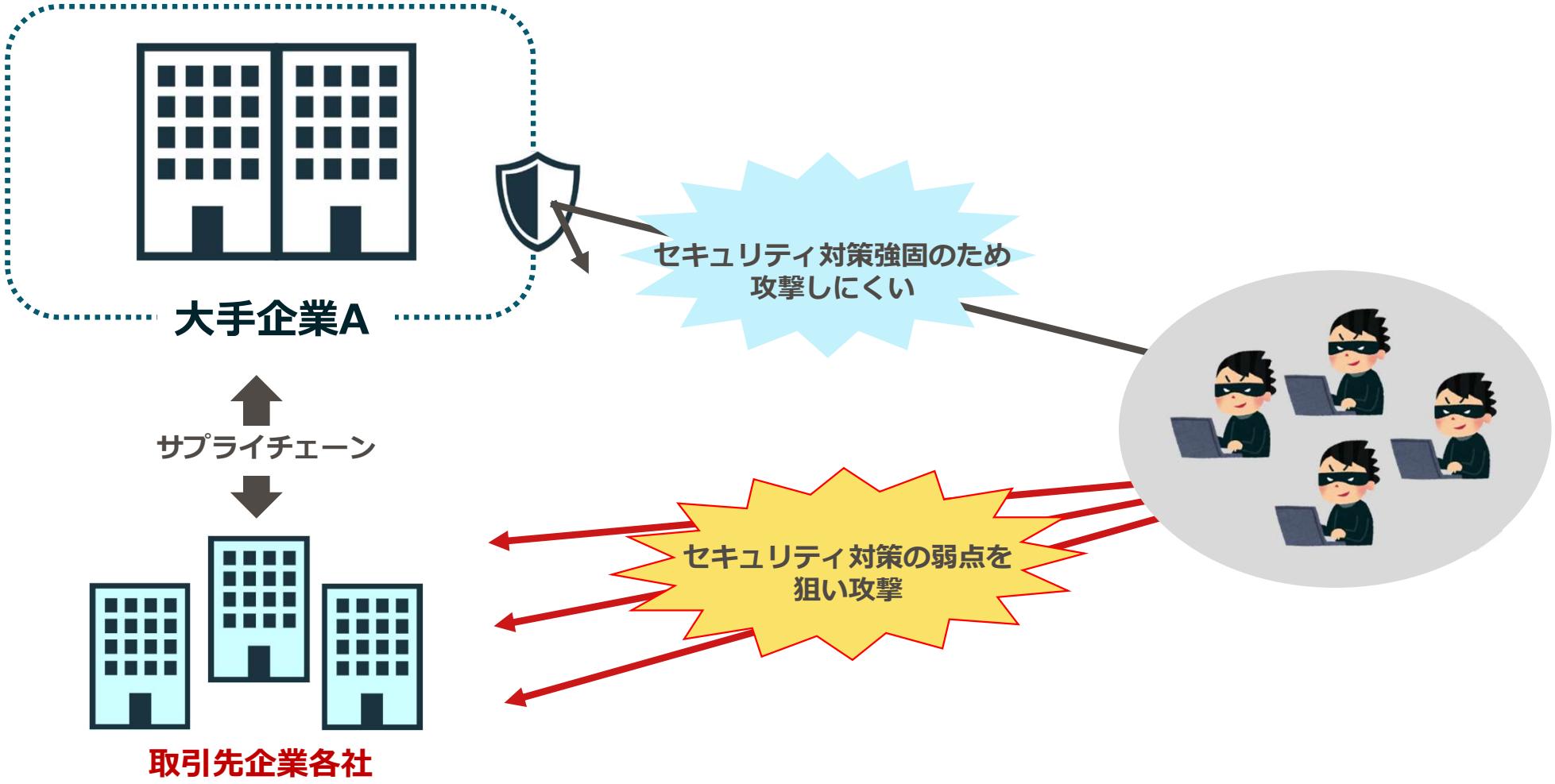
■2022年10月

病院の入院患者用の食事を提供するために**委託していた給食業者のシステム内に侵入**し、窃取した病院のサーバ認証情報を用いて、**病院内の給食サーバーに侵入**し、他の主要なシステムにも次々とランサムウェアの感染を拡大させた。
同病院のサイバー攻撃対策は、**境界防御に依存しており、院内のネットワークセキュリティは手薄**であったうえ、**病院システムのサーバー・端末では共通のパスワードを使用**しており、ログイン失敗時のアカウントロック等も行っていなかったため、容易に攻撃の横展開を許してしまった。
結果として、約６週間以上、同病院は電子カルテを含めた総合情報システムが使用できなくなり、外来診療や各種検査を行うことができなくなった。
システムの再開にあたっては、約2000台ものサーバー・端末を初期化し、クリーンインストールを行うとともに、今回指摘された脆弱性の改善を実施した。

出典：https://xtech.nikkei.com/atcl/nxt/column/18/00001/07877/
https://www.gh.opho.jp/important/785.html

サプライチェーン攻撃の背景

攻撃者の多くは、セキュリティ意識の高い大手企業を攻撃対象とはせず、その企業と取引のある企業のセキュリティ的な弱点を突いて攻撃を仕掛けます。



サプライチェーン攻撃に備えた対策

委託先などの企業も含め、自社の情報を取り扱う取引先には、自社と同等かそれ以上のセキュリティ対策を行っていることを確実にしておく必要がある。

自組織で行うべき被害の予防

■リスク低減のための措置（各種セキュリティ対策レベルの見直し）
本人認証の強化、最新セキュリティパッチの適用、従業員教育
■インシデントの早期検知
■インシデント発生時の適切な対処・回復

他社での取り組み事例

■チェックリストを用いて関係企業先の取り組み状況を緊急確認
■自組織内で普段から実施している対策の中で
特に留意すべきポイントを点検
■グループ全社への注意喚起とCSIRTによる対応手順を点検・確認

出典：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/activities/kougekiWG/images/info20220331.pdf

内部不正による情報漏えいへの注意点

近年、個人情報や機密情報を取り扱う担当者などによる不正な情報の持ち出し事案や職場環境の多様化によるリスクが増加しているため、注意が必要です。

企業における実施事項

- 内部規定において**秘密保持契約**を定め、就業規則で順守を求め、誓約書を提出させる
- 秘密保持の有効期間を在職中のみならず、**退職後についても適用**となるよう定める
- 定期的な**社員教育**の中に内部不正に関する注意喚起を含めている
- 経営層や管理層が内部不正の事業リスクを十分に認識し、優先度の高い経営課題として捉える
- 属人的、単独での作業などを実施しない**環境を整備**する

個人において注意すべきこと

- 個人情報や機密情報など**情報の資産価値や取扱いの注意事項を正確に理解**する
- 内部不正による自組織が被る**社会的・経済的な影響や、懲罰の内容を理解**しておく
- リモートワーク時などの外部脅威者からのアプローチに注意を払う

出典：IPA
【企業の内部不正防止対策に関する実態調査】
https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html
【組織における内部不正防止ガイドライン】
https://www.ipa.go.jp/security/guide/hjuojm00000055l0-att/ps6vr7000000jvcb.pdf

まとめ

・企業は様々なセキュリティ脅威にさらされている

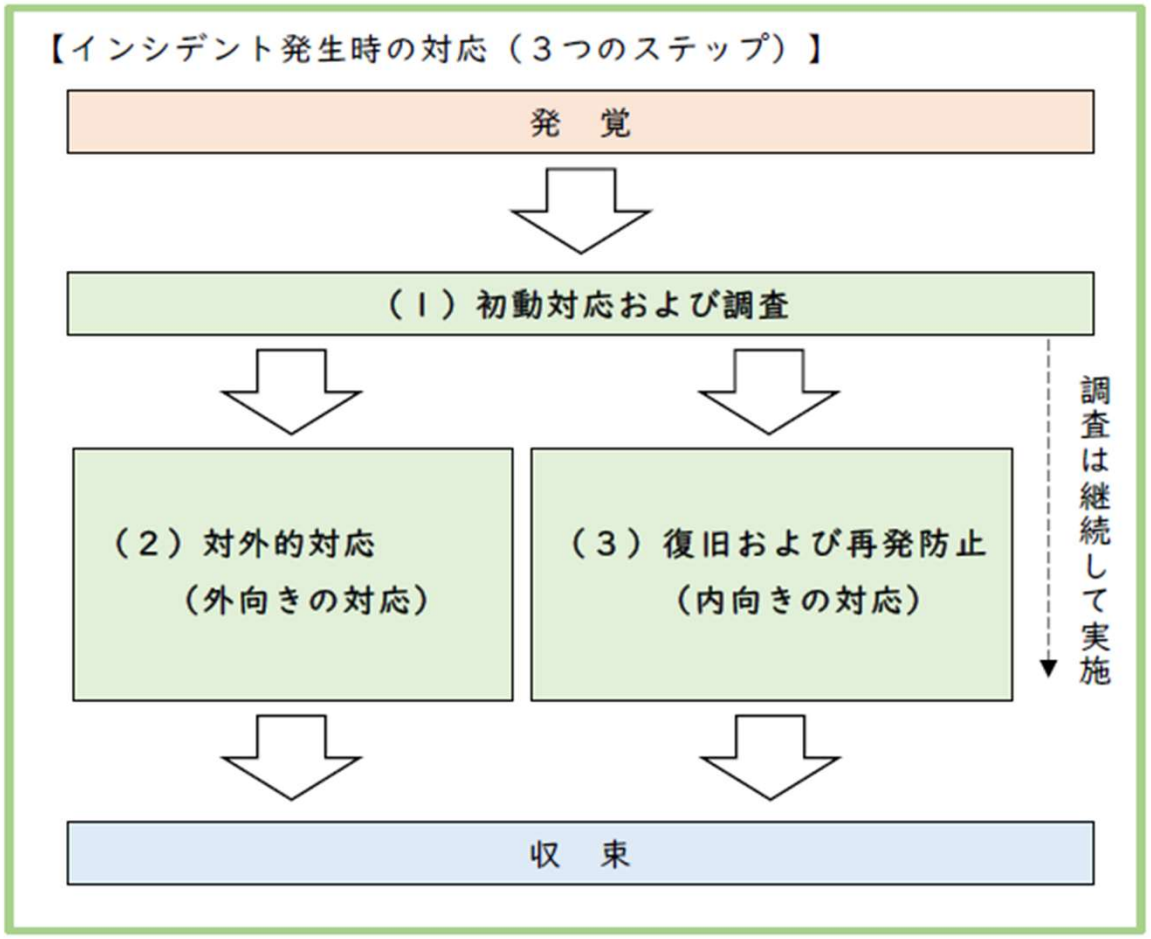
・特に被害が多い脅威はランサムウェア、サプライチェーンへの攻撃、内部不正

・その他にも様々な攻撃による被害が発生している

サイバー攻撃されたらどうなる？

インシデント発生時の対応と損害

サイバー攻撃を受け、それがインシデントへと至った際には、以下の様な企業としての対応、またそれに伴う各種損害の発生へとつながっていきます。

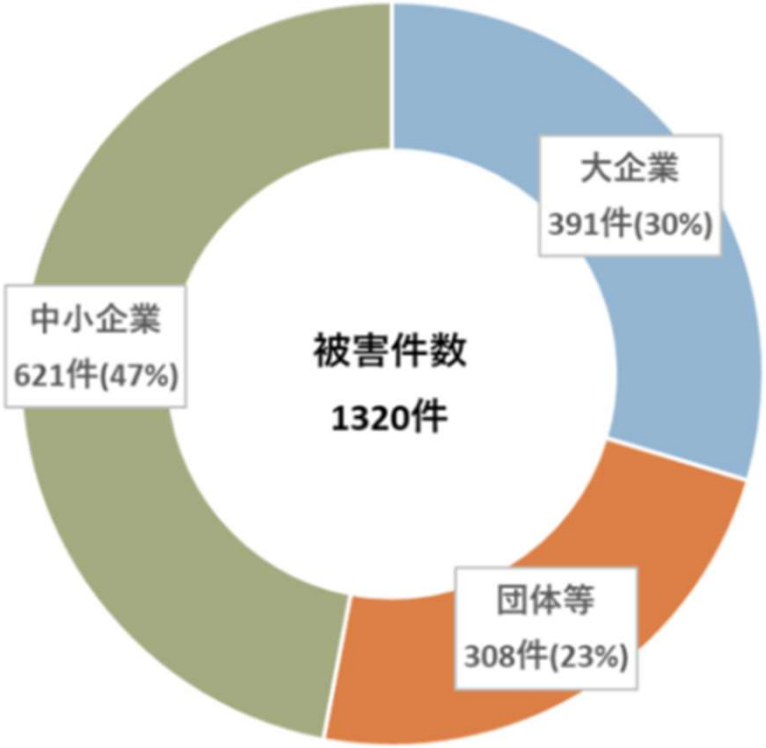


①費用損害(事故対応損害)
収束に向けた各種事故対応の負担により被る損害
②賠償損害
第三者からの損害賠償請求により被る被害
③利益損害
事業中断した場合の利益損失、固定費支出等
④金銭損害
脅迫などにより発生した直接的な金銭被害
⑤行政損害
個人情報保護法、GDPR等の違反による課徴金等
⑥無形損害
風評被害、ブランドイメージの低下等

出典：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/202402.html

サイバー攻撃による被害

■サイバー攻撃対象内訳



◆対象期間
2017年1月から5年半

◆被害規模(平均)
・ランサムウェア
-金額：2,386万円
-対応工数：27.7人月

・Emotet(エモテット)
-金額：1,030万円
-対応工数：2.7人月

・ウェブサイトからの情報漏洩
-金額：2,955万円
-対応工数：13.3人月

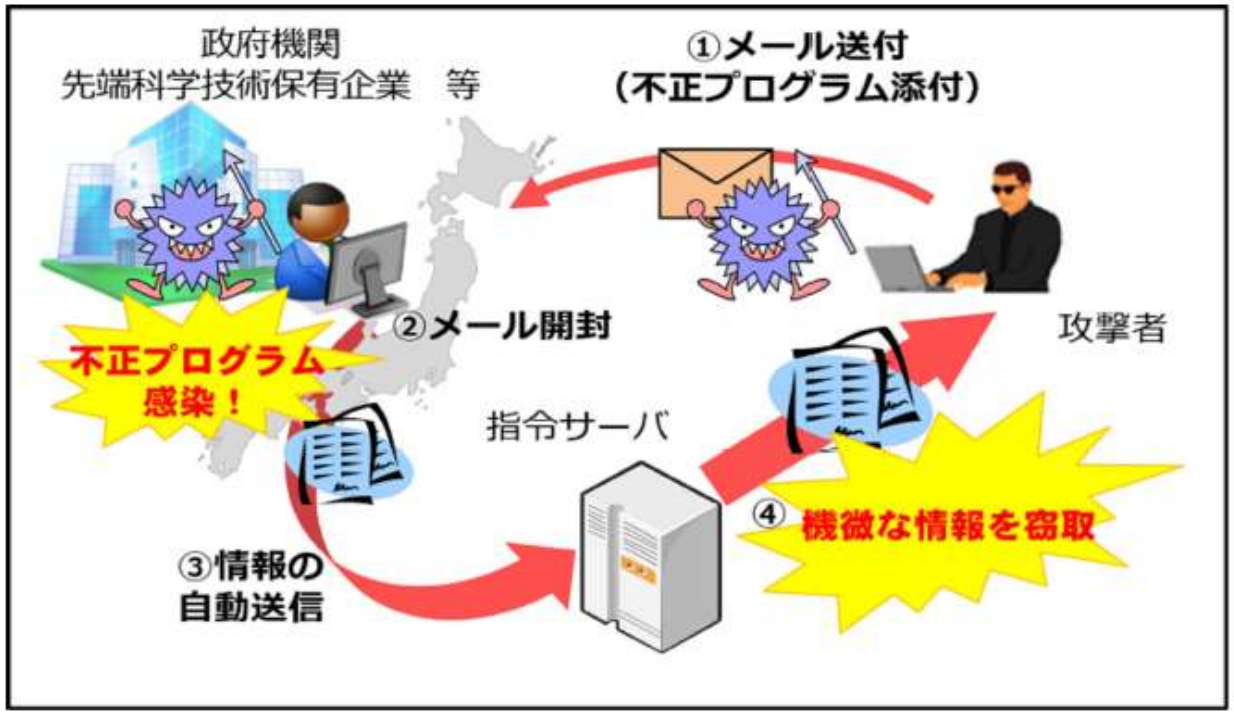
・ランサムウェアの被害については全て1000万円超の回答
・エモテットについては極端に少額の回答もあり
・ウェブサイトから漏洩した情報にクレジット情報が含まれる場合、金額、対応工数共にさらに増加する

出典：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/202402.html

標的型攻撃メールの手口

- **「ばらまき型」攻撃により不特定多数のメールアドレスに対して攻撃が行われる。**

【標的型メール攻撃の概要】



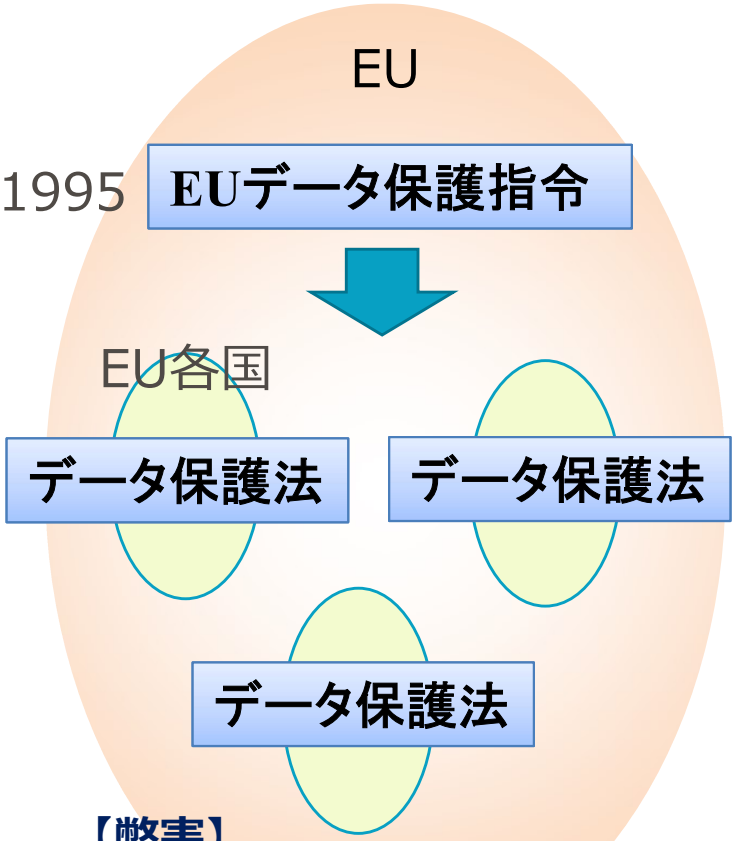
多数が非公開メールアドレスに対する攻撃であり多くの攻撃において送信元メールアドレスを偽装している。

出展　警察庁「平成30年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_cyber_jousei.pdf

EMOTET：標的型攻撃など主にメールにより感染するマルウェア。
感染すると端末を遠隔操作されると共に、メール情報から既存のやり取りに類似したメールへと進化していく特徴を持つ。

【参考】一般データ保護規則（GDPR）

EUでは、2018年5月にEUデータ保護指令が廃止され、一般データ保護規則に移行して、EU域内均一化とプライバシ保護を強化



【弊害】
- **法律の内容にバラつき**
- **データ移転許可手続きも各国毎**

EU

一般データ保護規則

2018年5月25日施行

個人の権利保障を強化する５つの特徴
- 消去権（忘れられる権利）
- データポータビリティ
- 知る権利
- プライバシー・バイ・デフォルト
- **巨額の制裁金**
  （全世界年間売上高の4%以下または2000万ユーロ以下）

【効果】
- **EU域内で均一化**

出所　http://www.iij.ad.jp/global/column/column44-1.html
http://itpro.nikkeibp.co.jp/atcl/column/16/021800039/021800001/?rt=nocnt
https://business.bengo4.com/category3/article27

個人情報関連のセキュリティインシデント

最近発生した情報漏洩等のインシデント事例の一部を以下に示す。

年月	企業等	概要
2023年4月	自動車製造　T社	自動車の車載インターネットサービスにおいて、**約215万人分の関連データ**（車載器ごとの識別番号である車載端末ＩＤ、車体番号、車両の位置情報、時刻等）が、10年近くにわたり外部から閲覧できる状態であったことを公表した。同サービスは、子会社に管理を委託しており、**クラウド環境の設定に誤り**があり、公開状態になっていた。
2023年4月	旅行業界　K社 （再委託先）	東京都の新型コロナウイルス感染者の管理システムにおいて、陽性者登録センターを受託しているK社の**再委託先に派遣された従業員**によって、システムにアクセスし、業務とは関係のない37人に関する**個人情報（氏名、住所、電話番号など）を興味本位で閲覧**し、メモにとり自宅に**持ち帰り、知人に送信**していた。他の従業員からの告発により事態が発覚し、派遣元事業者では、当該従業員を懲戒解雇した。
2023年3月	自動車販売業者　Ｉ社	I社において、同社サーバがランサムウェアに感染し、保有する個人情報が外部に流出した可能性があることを公表した。同社によると、**第三者からの不正アクセスを受け、サーバがランサムウェアに感染**し、一部業務システムの起動ファイルが暗号化された。 個人データが外部に送信された痕跡は無いものの、**240万2233件の個人情報が攻撃者によって参照**された恐れがあることを確認した。
2023年1月	通信販売業　O社	通販サイトにおいて、**システムに存在する脆弱性を突く不正アクセス**を受け、決済アプリケーションの改ざんなどが行われ、顧客情報（任意で入力した会社名や生年月日も含む）の最大約4900人分が盗まれた。また、同サイトで決済した**1830人分のクレジットカード情報**（名義、番号、有効期限、セキュリティコード）が**流出**し、窃取された可能性があると公表した。 なお、本件はクレジットカード会社による情報流出の可能性についての連絡から被害が発覚した。
2022年2月	N市役所	市内にある病院にて、退職した元職員が後輩職員へ業務マニュアルを見たいと話し、患者の**個人情報（氏名、住所、生年月日、医療情報、家族情報など）を不正に入手**し持ち出した。 元職員は、**他医療機関で治療することを勧誘する目的**で使用した。退職時にどのような秘密保持契約を交わしていたかは、不明。同院は患者への説明・相談窓口の設置と、内閣府の個人情報保護委員会への連絡、警察へ告訴した。

出典：securityNEXT(http://www.security-next.com/)

まとめ

・セキュリティインシデントは企業規模によらず発生している

・その被害は決して小さいものではない

・攻撃はより簡単に、より多くの目的達成が可能な形で行われる

中小企業のセキュリティ対策はどうしたら良いか？

セキュリティを守るための三要素

- **セキュリティを守るためには、以下の三要素をバランス良く確保することが必要です**

機密性 見るべき人が見れて、見てはいけない人が見れないこと

完全性 見るべき人が見れる情報は、いつでも正しい情報であること

可用性 見るべき人が必要なものをいつでも見れること

質問

質問：みなさまはそれぞれの物品への盗難・紛失・破損等のリスクに対してどのような対策を行いますか？

数万円の備品類

数千万円の設備

数万円の備品

・施錠等の一般的な盗難対策

・そもそも対策を行わない

etc

数千万円の設備

・保険への加入

・部品等、修理用の備品確保

etc

保護する対象の価値によって対策は異なる

⇒保有する情報資産の価値に応じて、必要な対応を実施すべき

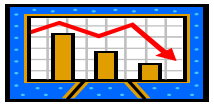
リスク分析・評価支援とは

企業における**組織の現状把握**として、考えられるセキュリティリスクを正しく評価する事で、適切なセキュリティ対策を定めていく事が出来ます

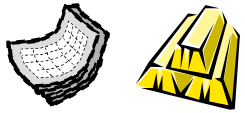
【リスク分析・評価とは？】

保護すべき情報や資産を明らかにし、脅威が発生した場合の損失（＝リスク）を分析し適切な対策を決定すること。

リスク ＝ **資産価値** × **脅威・攻撃** × **脆弱性**



脅威が発生した際にもらされる損失・被害



情報や資産の価値

情報/資産への攻撃

対策の抱える弱さ

リスク（損失）の大きさと、対策にかかる費用・稼動等を比較検討し、実施すべき対策、改善すべき対策を決定する。

手順書や作業で使用する帳票のサンプルを提供

①～④の全社共通の手順の策定。

手順に従い、リスク分析を実施

①資産の明確化

②脅威の分析

③リスクの評価

④対策の見直し

既存の対策・手順の活用を前提に、改善案等を提案

状況を正しく把握する⇒本格的なセキュリティ対策の入り口

中小企業の情報セキュリティ対策ガイドライン(STEP3,4)

出典：IPA 中小企業の情報セキュリティ対策ガイドライン　第3.1版
https://www.ipa.go.jp/security/guide/sme/about.html

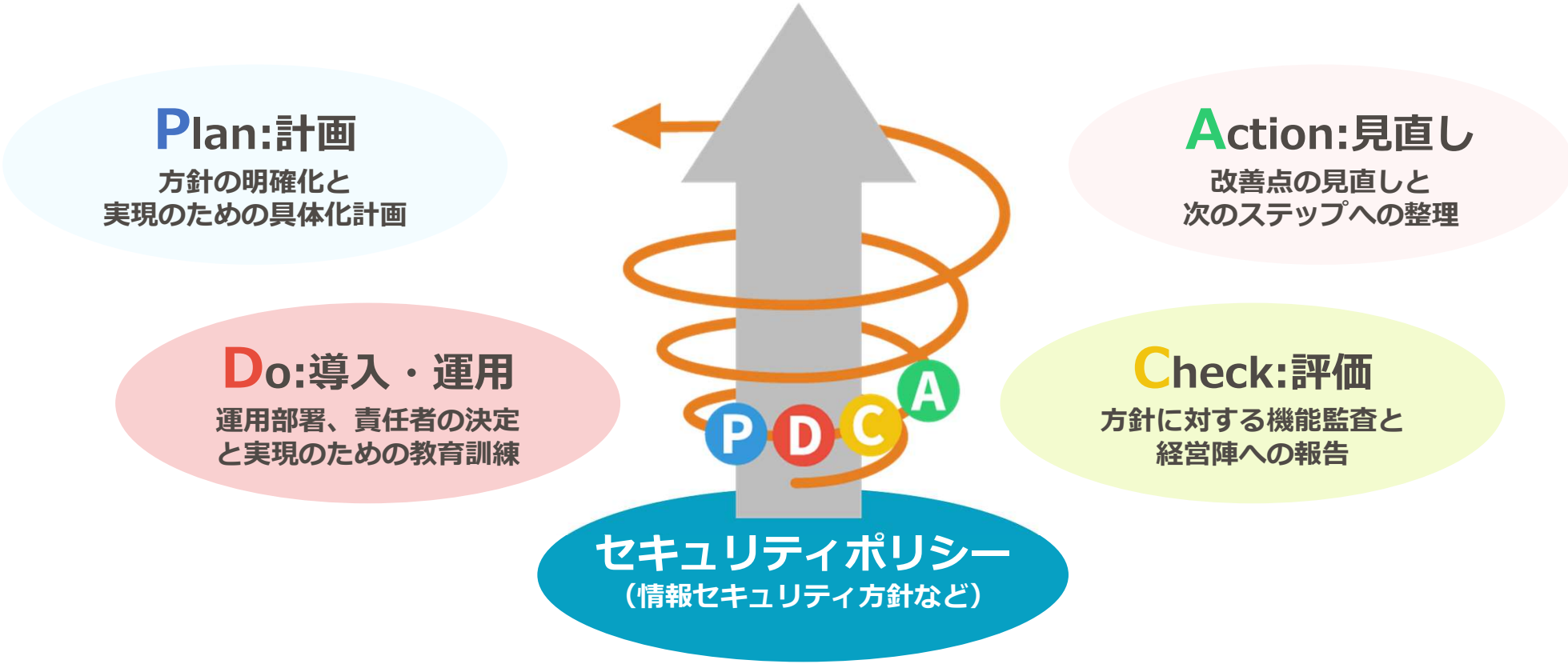
取組状況とアクション	本ガイドラインの活用方法
Step1 まず始めましょう	これまで情報セキュリティ対策を特に意識していない場合は**「2. できるところから始める」**(P.19) を参照して、「情報セキュリティ 5 か条」を実行してください。 進め方 「情報セキュリティ 5 か条」を社内で配付するなど、まずできるところから開始してください。
Step2 現状を知り改善しましょう	Step1 は実施できていて次に進める場合は **「3. 組織的な取り組みを開始する」**(P.20) を参照して、「5 分でできる！情報セキュリティ自社診断」で自社の状況を把握し、できていない対策の実行に努めてください。 進め方 ・「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成してください。 ・「5 分でできる！情報セキュリティ自社診断」で現状の対策を把握し、実施すべき対策を検討してください。 ・「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知してください。
Step3 本格的に取り組みましょう	Step2 までは実施できていて次に進める場合は **「4. 本格的に取り組む」**(P.24) を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。 進め方 ・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。 ・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に規程を作成してください。 ・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。
Step4 改善を続けましょう	**「5. より強固にするための方策」**(P.32) を参照して、自社に必要な対策を追加実施してください。Step1 や Step2 に取り組んでいる企業でも、Step4 を参照して必要な対策があれば実行してください。

ISMS認証制度等 (ISO27001) ←

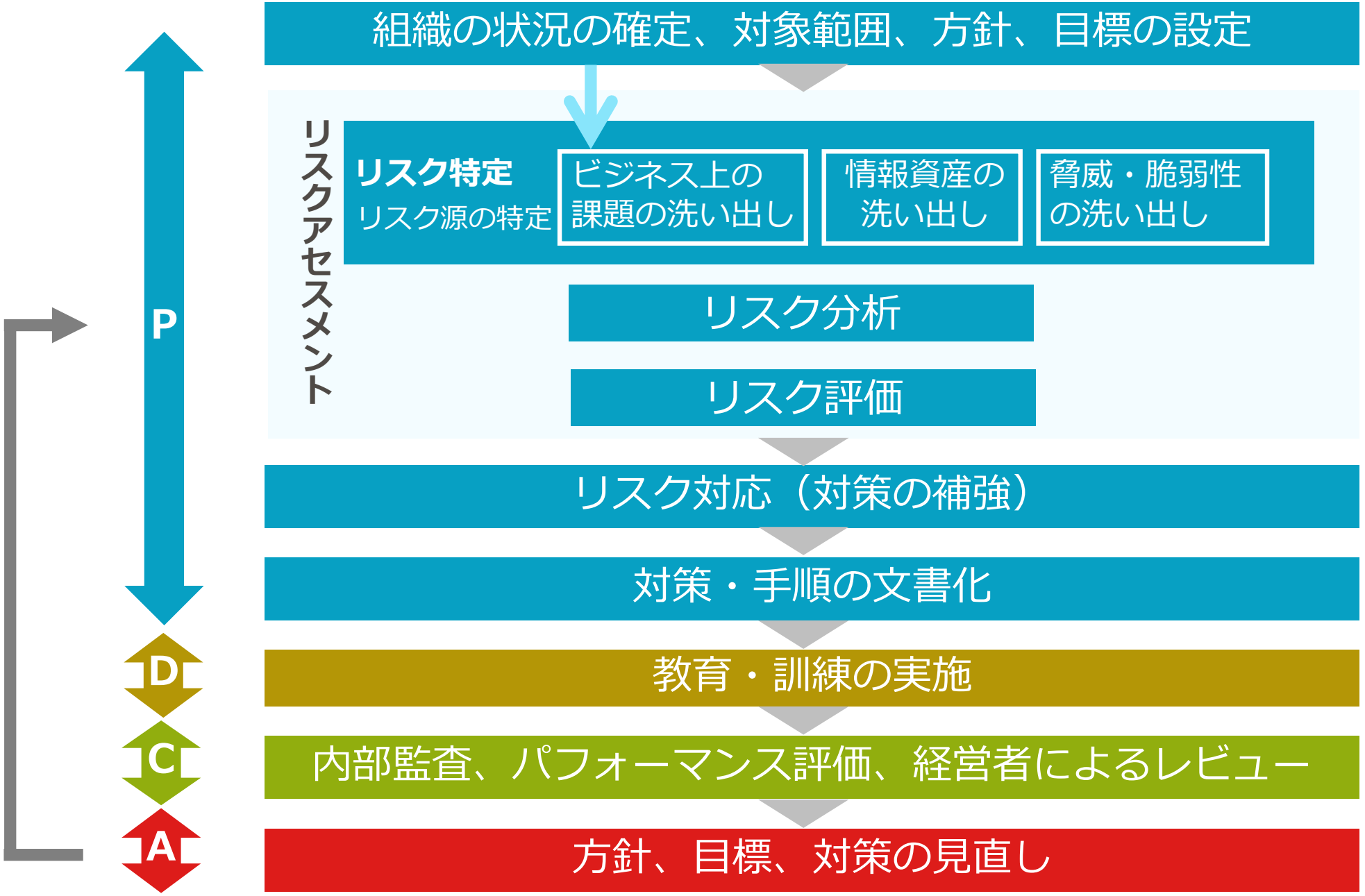
ISMS(情報セキュリティマネジメントシステム)とは？

Information Security Management System:情報セキュリティマネジメントシステム

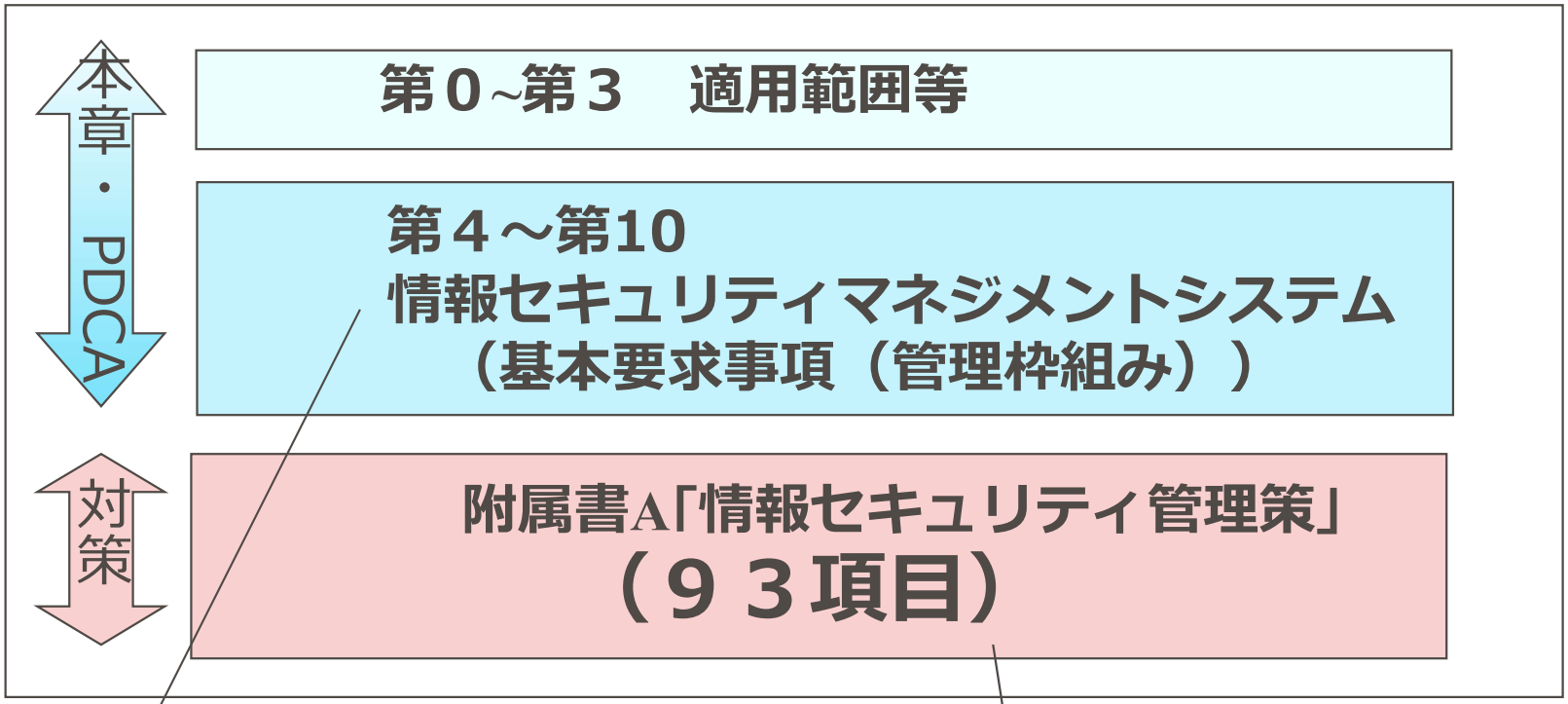
PDCAサイクルをまわし続ける（スパイラルアップ）ことで、
セキュリティを維持・**継続的に改善**すること



ISMSのPDCA



ISMS認証基準（ISO27001）の構成



改善のＰＤＣＡのための基本要求事項
（方針・目標設定、リスク分析、文書管理、
内部監査、是正など）

脆弱性の補強のための標準的な対策集
（入退管理、ＩＤパスワード管理、バックアップ、
運用・復旧の手順化など）

【参考】ISO/IEC 27001とISO/IEC 27017の関係

ISMSをベースとしたアドオン認証

ISMS（ISO/IEC 27001）認証取得を前提として、**クラウドサービス**の情報セキュリティ規格（ISO/IEC 27017）を満たしている組織を認証する仕組み

2016年8月に制度開始

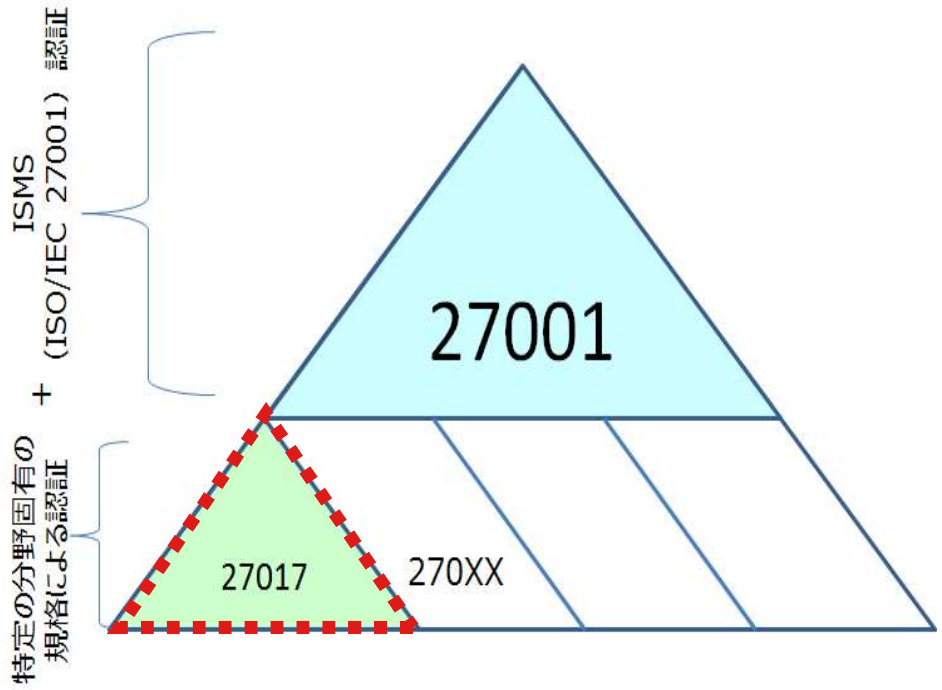


図　アドオン認証のイメージ

ISO/IEC27017を
取得するには、**ISMS**を取得する
ことが条件

従来の27001ベースの管理策

＋

クラウド固有のリスクを考慮
した27017ベースの管理策

参考：JIPDEC　「ISMSクラウドセキュリティ認証」
https://isms.jp/isms.html

中小企業の情報セキュリティ対策ガイドライン(STEP1,2)

出典：IPA 中小企業の情報セキュリティ対策ガイドライン　第3.1版
https://www.ipa.go.jp/security/guide/sme/about.html

取組状況とアクション	本ガイドラインの活用方法
Step1 まず始めましょう	これまで情報セキュリティ対策を特に意識していない場合は**「2. できるところから始める」**(P.19) を参照して、「情報セキュリティ 5 か条」を実行してください。 進め方 「情報セキュリティ 5 か条」を社内で配付するなど、まずできるところから開始してください。
Step2 現状を知り改善しましょう	Step1 は実施できていて次に進める場合は **「3. 組織的な取り組みを開始する」**(P.20) を参照して、「5 分でできる！情報セキュリティ自社診断」で自社の状況を把握し、できていない対策の実行に努めてください。 進め方 ・「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成してください。 ・「5 分でできる！情報セキュリティ自社診断」で現状の対策を把握し、実施すべき対策を検討してください。 ・「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知してください。
Step3 本格的に取り組みましょう	Step2 までは実施できていて次に進める場合は **「4. 本格的に取り組む」**(P.24) を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。 進め方 ・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。 ・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に規程を作成してください。 ・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。
Step4 改善を続けましょう	**「5. より強固にするための方策」**(P.32) を参照して、自社に必要な対策を追加実施してください。Step1 や Step2 に取り組んでいる企業でも、Step4 を参照して必要な対策があれば実行してください。

Security Action(情報セキュリティ5か条)

■サプライチェーン強化に向けたセキュリティ対策評価制度

	三つ星（★3）	四つ星（★4）	五つ星（★5）
	・ ビジネス観点（データ保護、事業継続）及びシステム観点で取引先を評価し、重要度に応じて★3/4/5に区分		
(1) 対象事業者のイメージ	・原則としてサプライチェーンを形成するすべての者	・ビジネス観点：重要度中　または ・システム観点：接続あり	・ビジネス観点：重要度大
(2) 対策の適用範囲（組織、システム）	・組織的対策 ・システム的対策（自社IT基盤）	・組織的対策 ・システム的対策 （自社IT基盤に加えて、発注者内部NWへの接続点）	追加の組織的対策は無し（★4取得が前提） ・システム的対策 （自社IT基盤への高度な対策上乗せ、OT等業務システムへの対策の追加）

■Security Action

★★二つ星

使用要件

「５分でできる！情報セキュリティ自社診断」の実施と、情報セキュリティ基本方針を定め、外部に公開したことを宣言

自社診断項目
- **Part1. 基本的対策（＝情報セキュリティ5か条）**
- **Part2. 従業員としての対策（13項目）**
  （情報の持ち出し対策、バックアップ取得等）
- **Part3. 組織としての対策（7項目）**
  （従業員へのセキュリティ教育等）

★一つ星

「情報セキュリティ5か条」に取組むことを宣言

情報セキュリティ5か条
1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

出典：経済産業省　第２回サイバーセキュリティ研究会ワーキンググループ１（制度・技術・標準化）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/002.html

出典：SECURITY ACTION
https://www.ipa.go.jp/security/security-action/

5分でできる！情報セキュリティ自社診断


診断編

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	-1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1は最新の状態にしていますか？	4	2	0	-1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	-1
	4	重要情報※2に対する適切なアクセス制限を行っていますか？	4	2	0	-1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	-1
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	-1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	-1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	-1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	-1
	10	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？	4	2	0	-1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	-1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	-1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	-1
	14	離席時にパソコン画面の覗き見や許可なき操作ができないようにしていますか？	4	2	0	-1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	-1
	16	退社時にノートパソコンや機密を施錠保管するなど盗難防止対策をしていますか？	4	2	0	-1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	-1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	-1
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	-1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	-1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	-1
	22	重要情報の授受を行う取引先との契約書には、秘密保持条項を設定していますか？	4	2	0	-1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	-1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	-1
	25	情報セキュリティ対策（上記 1～24 など）をルール化し、従業員に明示していますか？	4	2	0	-1

※1 コンピュータウイルスを検出するためのデータベースファイル（パターンファイル）とも呼ばれます。
※2 重要情報には営業秘密など事業に必要で価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のことです。

診断の後は次ページ以降を読んで対策を検討してください。

A+B+C 合計 点

3

・Part1
基本的な対策：全5項目
(＝情報セキュリティ５か条)

・Part2
従業員としての対策：全13項目

・Part3
組織としての対策：全7項目

合計：25項目

全て対応してSTEP2が完了

出典：IPA　https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf

自社診断項目サンプルと対応例

■従業員としての対策

- 電子メールやFAXの宛先の送信ミスを防ぐ取り組みを行っていますか？

(対応例)⇒他社員によるクロスチェック、送信先データの事前登録等による誤入力防止等

■組織としての対策

- 従業員にセキュリティに関する研修や注意喚起を行っていますか？

(対応例)⇒業務ミス防止のための注意事項の取りまとめ、事業所の壁などへの注意事項の掲載等

情報セキュリティ5か条への対応

■情報セキュリティ５か条
１．OSやソフトウェアは常に最新の状態にしよう！
２．ウィルス対策ソフトを導入しよう！
３．パスワードを強化しよう！
４．共有設定を見直そう！
５．脅威や攻撃の手口を知ろう！

１．WindowsUpdateの実施、サービスHPでのアップデート情報の定期的な確認
２．有償ソフト導入,Windowsセキュリティの有効活用
３．PW桁数最小値の設定、複数種類文字の利用
４．共有IDの廃止、IDの権限設定、PW管理の厳格化
５．IPAのHP等による情報収集、セミナーや勉強会への

まとめ

・必要な対応は企業の保有資産の価値によって変わってくる

・一般的な対応としてはISMS等に代表されるセキュリティフレームに沿った対策を進めること

・少なくとも最小限の実施可能な対応は推奨されている

さいごに

・本日のセミナー参加でもセキュリティ対策の一部となっています。まずは意識するところから

・セキュリティ対策に対策を重ねた結果、その負荷が課題になっている企業様も数多くいらっしゃいます

・対策はできる所から、その後、持続可能な範囲でのセキュリティ対策の強化を推奨いたします

お問合せ先

お問い合わせ(全般)
ＮＴＴテクノクロス株式会社
セキュアシステム事業部
第三ビジネスユニット
営業担当：田村　基樹
問合せ先：tamura.motoki@ntt-tx.co.jp
TEL：080-1033-6457

ご清聴ありがとうございました