参考資料1

（参考資料１）民間企業におけるゼロトラスト導入事例

ゼロトラスト導入事例－導入背景サマリ－

参考資料1

インターネットにてゼロトラスト導入事例が公開されている民間企業の導入事例を23事例調査を実施した。
そのうち、ゼロトラスト導入に至った導入背景の内訳は下記のとおり。

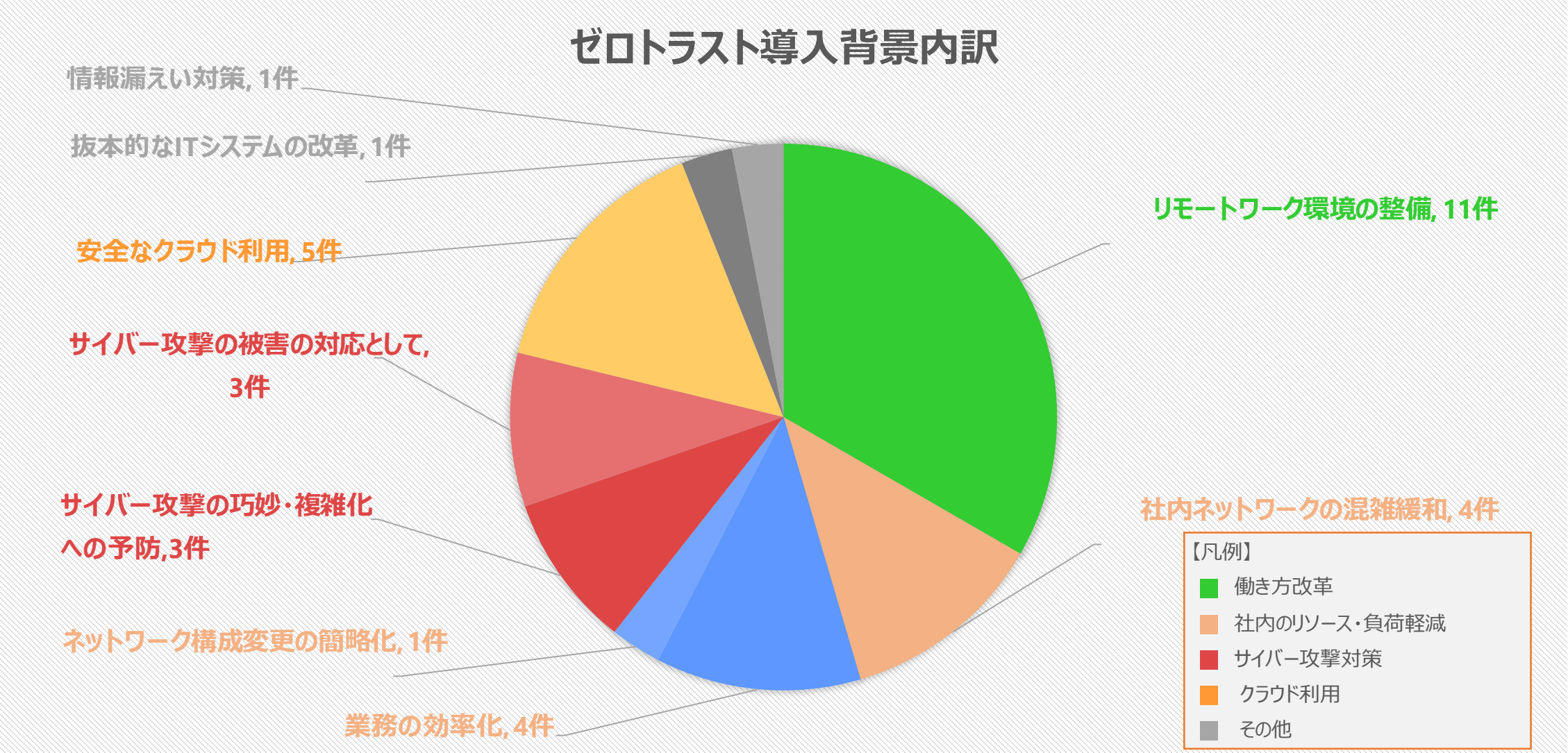
No.	導入背景	区分	該当事例件数(件) ※
1	リモートワーク環境の整備	働き方改革	11
2	安全なクラウド利用	クラウド利用	5
3	社内ネットワークの混雑緩和	社内のリソース・負荷軽減	4
4	業務の効率化	社内のリソース・負荷軽減	4
5	サイバー攻撃の巧妙化・複雑化への予防	サイバー攻撃対策	3
6	サイバー攻撃の被害の対応として	サイバー攻撃対策	3
7	ネットワーク構成変更の簡略化	社内のリソース・負荷軽減	1
8	抜本的なITシステムの改革	その他	1
9	情報漏えい対策	その他	1
10	導入背景の記載なし	その他	1

※ 調査事例の中には、複数導入背景の記載があったため、
調査事例数より導入背景の件数が多い

ゼロトラスト導入事例－導入背景サマリ－

参考資料1

前述した結果を円グラフにまとめたものは下記のとおり。



ゼロトラスト導入事例記事一覧（1/2）

参考資料1

ゼロトラスト導入事例の出典元記事は以下の通り。

No.	導入背景	記事名	掲載元
1	• 業務の効率化 • リモートワーク環境の整備	多数のツールでゼロトラストを構築するauカブコム証券、2つのSIEMを使う理由	日経クロステック【IT】
2	• ネットワーク構成変更の簡略化	大和証券がゼロトラスト推進、「SWG」で従業員のネット利用を社内外問わず保護	日経クロステック【IT】
3	• 抜本的なITシステムの改革 • リモートワーク環境の整備	IT業務効率化に舵を切るSOMPO、SSC導入とセキュリティ対策のリアルを聞く	マイナビニュース
4	• 社内ネットワークの混雑緩和	テレワーク急増もOK　秘密は「脱VPN」（LIXIL）	日経クロステック【IT】
5	• サイバー攻撃の被害の対応として	富士フイルムが本気のゼロトラスト　EDRとSIEMに続き、SASEも導入予定	日経クロステック【IT】
6	• 安全なクラウド利用 • 社内ネットワークの混雑緩和	カシオ計算機がゼロトラストを推進、DX向けシステム開発の安全性を高める仕組み	日経クロステック【IT】
7	• 業務の効率化 • リモートワーク環境の整備	ゼロトラストでグローバルのセキュリティとコミュニケーションを同時に効率化：「海の向こう」もセキュアに、クリアに（JX金属）	ITmedia
8	• リモートワーク環境の整備 • 社内ネットワークの混雑緩和 • ネットワーク構成変更の簡略化	全世界5万人が在宅勤務　VPN渋滞とも無縁（武田薬品工業）	日経クロステック【IT】
9	• リモートワーク環境の整備	ゼロトラストの本質はビジネスに価値をもたらすこと――アサヒグループジャパンの取り組みと、マイクロソフトの統合セキュリティ対策スイートへの期待	マイナビニュース
10	• サイバー攻撃の巧妙化・複雑化への予防 • 安全なクラウド利用	NECの社内DXの1年、「小さな成功」を目標に230プロジェクトで変革目指す	マイナビニュース
11	• 社内ネットワークの混雑緩和 • 業務の効率化	旭化成、ゼロトラストの実現に向けてSD-WANとSIGを用いた新WAN環境を導入	ITmedia

上記の導入事例は有料記事等を参考に調査しており、著作権等の都合上記事名のみの記載とする。

ゼロトラスト導入事例記事一覧（2/2）

参考資料1

ゼロトラスト導入事例の出典元記事は以下の通り。

No.	導入背景	記事名	掲載元
12	• リモートワーク環境の整備	半年で全社のセキュリティを「ゼロトラスト」に古河電工の情シスが語る、現場と経営陣の巻き込み方	ITmedia
13	• サイバー攻撃の巧妙化・複雑化への予防	オープンハウスがセキュリティー対策強化、XDRやSWGによる多層防御を目指す	日経クロステック【IT】
14	• 安全なクラウド利用	全業務システムをSaaS群で構成するトリドール、変化対応へ求めた3つの要件	日経クロステック【IT】
15	• リモートワーク環境の整備	約1年半で「脱・境界型セキュリティ」を実現――ZOZOグループに導入プロセスと運用について聞いてみた	Darsana
16	• リモートワーク環境の整備	鴻池運輸が業務システムの9割をクラウド移行、4年をかけた成果	日経クロステック【IT】
17	• サイバー攻撃の巧妙化・複雑化への予防 • 情報漏えい対策 • 安全なクラウド利用	ゼロトラストネットワークの実現に向けて――Microsoft 365 E5 で整備した包括的なセキュリティ体制のもと、ポケモンというコンテンツを "安全" "安心" に提供し続ける	マイナビニュース
18	• サイバー攻撃の被害の対応として	横の動きをつかめ　NTTコムの教訓	日経クロステック【IT】
19	（導入背景の記載なし）	国内事例に学ぶゼロトラスト導入、第一歩となるアクセス制御の工夫とは（シスコシステムズ）	日経クロステック【IT】
20	• 業務の効率化	住友商事が次期コラボレーション基盤に Microsoft 365 E5 をグローバル採用! ゼロトラストセキュリティなど 3 つの成果を得る	マイナビニュース
21	• サイバー攻撃の被害の対応として • 安全なクラウド利用	EDRを起点にゼロトラストに挑む竹中工務店、ユーザーの使い勝手も向上したわけ	日経クロステック【IT】
22	• リモートワーク環境の整備	2週間で在宅勤務の環境構築 「ゼロトラスト」の思想取り入れる（同志社大学）	日経クロステック【IT】
23	• リモートワーク環境の整備	ゼロトラスト型リモートアクセスとタブレットで業務効率化と営業力強化を実現（仙台銀行） **※次ページ以降に要約を記載**	事業者公開情報

上記の導入事例は有料記事等を参考に調査しており、著作権等の都合上記事名のみの記載とする。

ゼロトラスト導入事例 –株式会社仙台銀行 –

参考資料1

ゼロトラスト型リモートアクセスとタブレットで業務効率化と営業力強化を実現

宮城県で営業する仙台銀行は、個人顧客向けサービス以外にも、法人顧客向けサービスの充実を図っている。法人向け営業力強化の方策の1つが、営業職員にモバイル端末を配布し、場所を問わずに社内システムにアクセスした業務を可能にすることだ。高いセキュリティが求められる金融機関のリモートアクセス環境として、ゼロトラストネットワークアクセス機能を備えた「IIJフレックスモビリティサービス/ZTNA」を導入。セキュアで安定したリモートアクセスにより、業務効率化と営業力強化を実現した。

導入前の課題

■ 営業力強化に向けてモバイル端末の必要性が高まる
- ✓ 行内だけの運用だったモバイル端末活用をいつでもどこでも働ける環境に拡大
- ✓ 渉外用タブレットは外から行内システムやファイルサーバーにアクセスできる必要がある
- ✓ 外部でモバイル端末を利用するためにはセキュリティや性能の担保が不可欠

選定の決め手

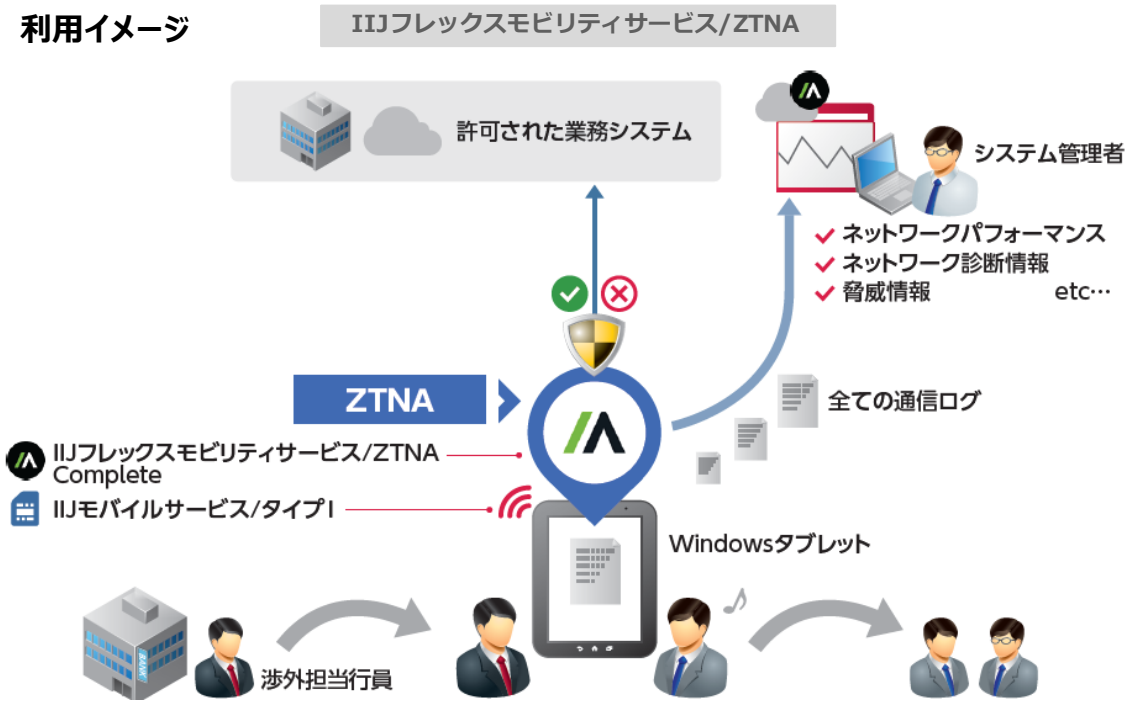
■ リモートアクセス環境構築に必要なことをワンストップで対応
- ✓ リモートアクセスとセキュリティのゼロトラスト機能が一体になっており、お客様のニーズに合致
- ✓ アクセス制御からゼロトラストに対応した管理まで含めたトータルパッケージとして対応可能
- ✓ 動作検証でリモートアクセス時のスピードを確認し導入へ

導入後の効果

■ 運用開始後はトラブルなく業務効率も向上
- ✓ 営業職員が行内に戻らず業務を遂行できるようになり業務効率の向上を実感
- ✓ IIJフレックスモビリティサービス/ZTNAは許容した内容や業務だけの通信に限定できるので、安心して使える
- ✓ 今後は渉外用タブレットを活用して業務改革を推進

※公開情報をもとに受託事業者が資料を作成

利用イメージ



導入したサービス・ソリューション

・IIJフレックスモビリティサービス/ZTNA　・IIJ Omnibusサービス
・IIJモバイルサービス/タイプI

・本記事は2022年12月に取材した内容を基に構成しています。記事内のデータや組織名、役職などは取材時のものです。
・会社名及びサービス名などは、各社の登録商標または商標です。

出典:IIJ社HP
https://www.iij.ad.jp/svcsol/case/sendaibank2.html

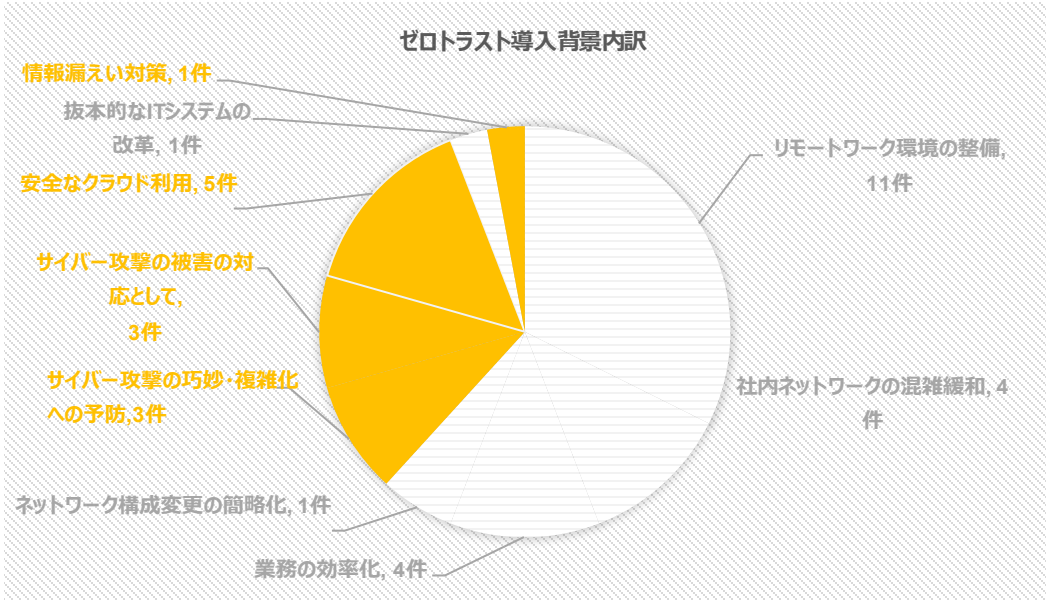
ゼロトラスト導入背景の分析

参考資料1

導入背景を調査した結果、サイバー攻撃の被害の対応及び予防や情報漏洩対策、安全なクラウド利用等のセキュリティの向上を考慮した理由からの導入が多く、具体的にはどのようなセキュリティインシデントが発生しているかについて詳細に調査を実施する。

No.	導入背景	区分	該当事例件数(件) ※
1	リモートワーク環境の整備	働き方改革	11
2	安全なクラウド利用	クラウド利用	5
3	社内ネットワークの混雑緩和	社内のリソース・負荷軽減	4
4	業務の効率化	社内のリソース・負荷軽減	4
5	サイバー攻撃の巧妙化・複雑化への予防	サイバー攻撃対策	3
6	サイバー攻撃の被害の対応として	サイバー攻撃対策	3
7	ネットワーク構成変更の簡略化	社内のリソース・負荷軽減	1
8	抜本的なITシステムの改革	その他	1
9	情報漏えい対策	その他	1
10	導入背景の記載なし	その他	1

※ 調査事例の中には、複数導入背景の記載があったため、
調査事例数より導入背景の件数が多い

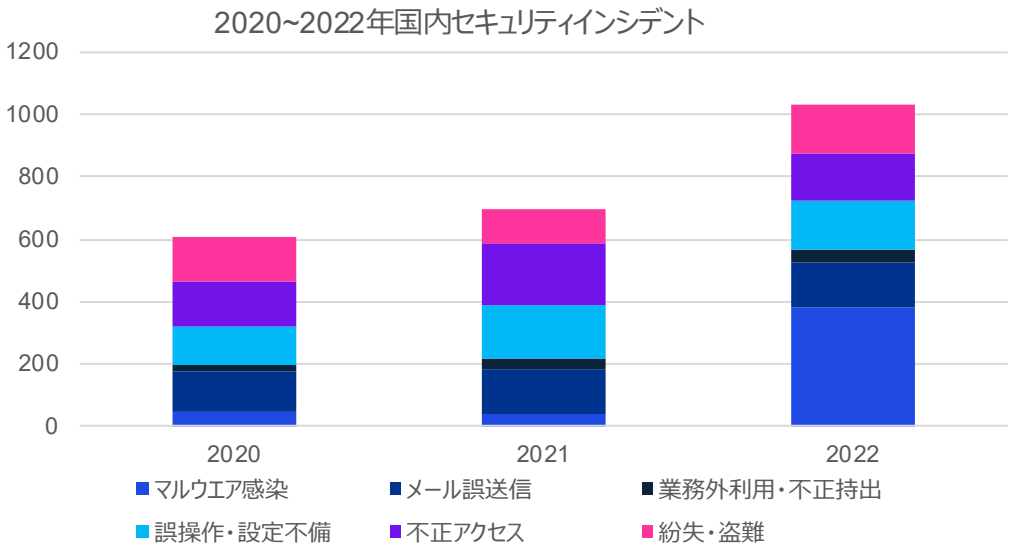


セキュリティ対策向上を目的にゼロトラストを導入する事例が多いため、具体的なセキュリティインシデントについて調査・分析を実施する。

セキュリティインシデント調査結果サマリ

参考資料1

セキュリティインシデントについて調査を実施。様々なインシデントが多数発生しており、ゼロトラストアーキテクチャを導入することによりセキュリティインシデントの解決・予防につながる。



『[2023年1月公開]過去3年分の国内セキュリティインシデント集計 | Digital Arts Security Reports | デジタルアーツ株式会社 (daj.jp)』を基に受託事業者作成

分類	主な事例（※）
不正アクセス	三和倉庫における不正アクセス
マルウェア感染	未知のランサムウェア感染
誤操作・設定不備	トヨタ自動車におけるクラウド環境の誤設定
紛失・盗難	兵庫県尼崎市におけるUSB紛失
業務外利用・不正持出	大阪府堺市の選挙データ流出
メール誤送信	福岡県職員によるメール誤送信

※次ページ以降に記載のインシデント事例より抜粋

これまでのゼロトラストアーキテクチャを導入することで様々なインシデント等の解決・予防につながる

不正アクセス
多要素認証等によって不正アクセスを抑制し、**EDRやSOCサービス**によって不正アクセスを検知する。

マルウェア感染
EDRやSOCサービスによる監視によって、未知のマルウェアによる攻撃を検知する。

誤操作・設定不備
CASBによる一貫したセキュリティポリシーの適用で設定不備を予防する。
CSPMによる設定不備を検知する。

紛失・盗難
MDMを利用することにより、デバイスを紛失した際に情報が閲覧されることを防止する。

業務外利用・不正持出
ユーザーの**ID・アクセス権限管理**によって、内部の不正による持出しを防止する。

メール誤送信
DLPを利用することにより、メール誤送信やファイル流出を防止する。

セキュリティインシデント事例－不正アクセス－（1/4）

参考資料1

不正アクセスの発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
1	アクセス制限解除による開発環境への不正アクセス	• 開発環境で、従来より実施していたアクセス制限を解除した際に、辞書攻撃による不正アクセスが発生。 • 保守用ネットワークの分離が不十分、管理者アカウントに推測容易なパスワードを設定していたため、複数のサービスに不正アクセスが広がった。	• CSIRTとPSIRTが定めるセキュリティ対策をもれなく実施 • 資産管理の方法を社内で明確に定義 • **ログの保存期間の見直し等サイバー攻撃検知のための対策**を実施	参考資料① P.21－P.24
2	グループ会社を経由した高度標的型攻撃	• 国内グループ拠点に標的型攻撃を受け社内に侵入された。 • 高度標的型攻撃であったため、既存のウイルス対策ソフトウェアでは検知できなかった。	• **グループ全体でEDR、NDRを導入** • 社内および顧客向けシステムの構成情報をあらかじめ登録し、公開された脆弱性情報に対するリスクを自動的に通知 • 保護すべき情報の優先度を決定し、優先度に応じた対策を実施	参考資料① P.25－P.28
3	総当たり攻撃による不正アクセス	• 利用しているクラウドサービスに、パスワード総当たり攻撃によって不正にアクセスされた。 • 機関内部システムにはクラウドサービスと同じID、PWを利用している利用者がおり、機関内部システムを踏み台にその他内部システムに不正アクセスされた。	• 認証システムの高度化を実施 • 情報の重要性に応じたネットワーク分離を実施し、職員の属性に応じて利用できるシステムを限定。 • **資産管理システムを導入**し、資産管理状況を把握し、IT機器の機能制御を実施。	参考資料① P.33－P.36
4	インターネットを経由した脆弱なアカウントを利用した不正アクセス	• インターネットに公開されていた検証用サーバに不要なアカウントが残存し、脆弱なパスワードが設定されていたことから不正アクセスされた。 • セキュリティ規定が十分に浸透しておらず、検証用サーバには脆弱なパスワード設定、機密情報が格納されていた。 • **EDR、ウイルス対策ソフトウェア、IDS等の多層防御を実施し運用体制も整備していたため、早期に侵入を検出し、被害を軽減できた。**	• 必要なセキュリティ対策が実施されるよう、組織・教育体制を強化 • CSIRT活動が円滑になるよう体制を整備	参考資料① P.37－P.40

※対象資料の再発防止策より一部抜粋

【参考資料】

• 参考資料① サイバー攻撃を受けた組織における対応事例集
kokai_jireishu.pdf (nisc.go.jp)

セキュリティインシデント事例 – 不正アクセス –（2/4）

参考資料1

不正アクセスの発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
5	インターネットを経由したなりすましによる不正アクセス	• 社外常駐者がインターネット経由で利用する社内システムの認証方式がパスワードのみであり、なりすましによって社内へ侵入された。 • ウイルス対策ソフトにより検知したが十分な分析ができなかったため、再度不正侵入が発生した。	• **認証方式強化のため多要素認証を導入** • **ウイルス検知や分析力向上のためEDRを導入し、MSS(※2)を契約**、IT部門を増員を実施 • 組織の実態に合わせて、情報セキュリティ関連規定の見直しを実施	参考資料① P.41 – P.44
6	VPN装置の脆弱性を悪用した不正アクセス	• オンプレミスとクラウド（AWS）上のサーバが不正アクセスを受け、サーバ内の一部のファイルが暗号化 • VPN装置の脆弱性を悪用され侵入された。 • サーバ内には攻撃者が設置したとみられる脅迫文が残されていた。	• 各種サーバの管理者アカウントの見直しとパスワードの複雑化 • 各種サーバのアクセス制限の見直し • **多要素認証の導入**	参考資料② P.38 – P.43
7	病院への閉域網を介した不正アクセス	• 病院がランサムウエアにより電子カルテなどが暗号化され、外来診療や各種検査を停止した。 • システムで使用されているサーバや端末では共通のパスワードを使用しており、アカウントロックも未設定であった。 • 病院の委託先である給食事業者のシステムと病院のシステムが閉域接続されおり、給食事業者システムにはリモート保守用FWが設置されていた。攻撃者はこのリモート保守用FWの脆弱性を突いて給食事業者のシステムに侵入し、閉域接続を過信しておりパスワード・アカウント設定等のセキュリティ対策が甘かったため、閉域網を通して病院のシステムまでランサムウェアを感染させた。	• セキュリティポリシーの整備によるパスワードの複雑化 • ベンダーと病院間での責任分界点を明確化し、脆弱性を残さない運用を整備	参考資料③

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料① サイバー攻撃を受けた組織における対応事例集 kokai_jireishu.pdf (nisc.go.jp)
- 参考資料② コンピュータウイルス・不正アクセスの届出事例［2022 年下半期（7 月～12 月）］ 000108764.pdf (ipa.go.jp)
- 参考資料③ 病院を襲ったランサムウエア攻撃の報告書が公開 病院を襲ったランサムウエア攻撃の報告書が公開 (nikkeibp.co.jp)

セキュリティインシデント事例 – 不正アクセス –（3/4）

参考資料1

不正アクセスの発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
8	三和倉庫における不正アクセス	• 2022年、三和倉庫のサーバがランサムウェアの攻撃を受け停止した。 • 攻撃者はVPN 機器の脆弱性を突いた攻撃によりネットワーク内部に侵入し、ドメインコントローラから認証情報を取得、複数のサーバから機密情報を盗み出し、同時にランサムウェアを実行した。	• 脆弱性への対策とアカウント棚卸を行い、**多要素認証を徹底** • ネットワークセグメントの構成を見直し、内部FWを設置 • **EDR、SOCの導入** • 内部から外部への不審な通信をブロックするURLフィルタリングを導入	参考資料④
9	カプコンにおける不正アクセス	• 2020年、カプコンのネットワーク上の機器がランサムウェアの攻撃を受け暗号化された。 • 攻撃者はカプコン北米法人の予備の旧型VPN装置から不正侵入し、機器から情報を窃取した。その後、機器にランサムウェアを感染させ、各機器内のファイルを暗号化した。	• **SOCサービスを導入**し、外部との接続を常時監視 • 不正な挙動およびコンピュータウイルス感染の早期検知のため、最新の**EDRを導入** • インシデント発生時の迅速な対処に向け、ログの長期保存などの管理方法を改善	参考資料⑤
10	産業総合研究所における不正アクセス	• 2017年から2018年にかけて、産総研の情報システムが継続的に外部から不正アクセスを受け、未公表の研究情報や、個人情報などが閲覧・窃取された。 • 攻撃者は外部レンタルサーバ上の研究用Webサイトを通じて、内部OSを遠隔操作し内部サーバを踏み台化。この踏み台サーバを介して、管理用ネットワーク内のサーバから職員のアカウントを窃取し、サーバ内の情報を閲覧・窃取した。	• 内部システムのログインに**多要素認証を導入** • 研究用ネットワークと業務用ネットワークを分離し、内部通信の監視を強化	参考資料⑥

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料④ 不正アクセスに関する調査結果のご報告
  35-0.pdf (sanwasoko.co.jp)
- 参考資料⑤ 不正アクセスに関する調査結果のご報告
  不正アクセスに関する調査結果のご報告【第4報】| プレスリリース | 株式会社カプコン (capcom.co.jp)
- 参考資料⑥ 産総研の情報システムに対する不正なアクセスに関する報告
  20180720aist.pdf

セキュリティインシデント事例 – 不正アクセス –（4/4）

参考資料1

不正アクセスの発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
11	SBI証券における不正アクセス	• 2020年、SBI証券の口座に対して、不正な出金や有価証券売却が行われた。 • 攻撃者は、SBI証券のメインシステムサイトに対して、何らかのリストを元にリスト型アカウントクラッキングにより不正ログインを実行した。	• ログイン及び出金指示等の特定の操作の認証手段として、**多要素認証を実装** • ログイン、出金指示、住所変更等のメール配信の対象となる手続きの拡充をはじめ、顧客への通知機能を強化	参考資料⑦
12	鳥取県鳥取市における不正アクセス	• 2020年、鳥取県鳥取市のふるさと納税サイトに対し不正アクセスが発生し、顧客情報や注文情報が流出した。 • 攻撃者は脆弱性診断ツールを悪用して、対象サイト内の脆弱性を発見し、数時間にわたりアクセスを繰り返しデータベース内の情報を搾取した。 • 当該サイトのユーザーに対してフィッシングメールが届く事象などの二次被害も発生している。	• 第三者機関へ脆弱性診断を実施 • システム脆弱性の修正 • システム監視体制の強化 • サイト内の管理権限の強化	参考資料⑧

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料⑦ 悪意のある第三者による不正アクセスに関する調査報告及び再発防止策について
  prestory210122_011800.pdf (sbisec.co.jp)
- 参考資料⑧ とっとり市・鳥取市ふるさと納税スペシャルサイトへの不正アクセスによる個人情報流出について
  saisyuhoukoku_20200706.pdf (tottori-ichi.jp)

セキュリティインシデント事例 – マルウェア感染 –（1/3）

参考資料1

マルウェア感染の発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
1	IoT機器の脆弱性を悪用した不正アクセス	• パッチ適用の必要性が認識されていなかったことや、パッチが適用できないIoT機器の脆弱性が残存していたことからランサムウェアが拡散した。	• セキュリティを統括する専門組織の設置やセキュリティ人材の教育を実施 • サイバー攻撃を踏まえたBCP対策や有事の訓練等を実施 • **資産管理（サーバの管理・識別）**を徹底 • **自前システムとゼロトラストソリューションのハイブリッド化の推進**	参考資料① P.9 – P.12
2	未知のランサムウェア感染	• 取引先を装ったメールの添付ファイルを従業員が開封したことで未知のランサムウエアに感染し、境界型防御をすり抜け企業内にまん延、ファイルサーバや業務サーバの大部分が暗号化された。 • 定義型のウイルス対策ソフトウェアに対策を依存していたため、未知のランサムウェアに侵入されると、被害を限定することが難しかった。	• **未知のマルウェアへの対策として、EDRを導入し、SOCサービスも契約** • インシデント発生時の対応手順を整備し、CSIRT整備にも着手 • オンプレミスサーバの被害を軽減するため、システムのクラウド移行や迅速な復旧のためのバックアップに関する見直しを実施	参考資料① P.13 – P.16
3	乗っ取られた取引先企業からの標的型メール攻撃	• 取引先企業のアカウントを乗っ取った攻撃者から、メールを受信した端末がマルウェアに感染。 • 既存のウイルス対策ソフトでは攻撃を検知できなかったが、**導入済みのEDRにより検知され、情報セキュリティ部門とベンダの迅速な連携により被害を軽減できた**。	• セキュリティ人材を各部門に配置しシステムのセキュリティのレビュー等を実施したり全社的にサイバー攻撃対策を実施 • 新たな脅威に対応するため、積極的な情報収集や新技術の導入を検討	参考資料① P.17 – P.20

※対象資料の再発防止策より一部抜粋

【参考資料】

• 参考資料① サイバー攻撃を受けた組織における対応事例集
kokai_jireishu.pdf (nisc.go.jp)

セキュリティインシデント事例－マルウェア感染－（2/3）

参考資料1

マルウェア感染の発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
4	閉域網を介した不正アクセス	• 病院がランサムウエアにより電子カルテなどが暗号化され、外来診療や各種検査を停止した。 • システムで使用されているサーバや端末では共通のパスワードを使用しており、アカウントロックも未設定であった。 • 病院の委託先である給食事業者のシステムと病院のシステムが閉域接続されおり、給食事業者システムにはリモート保守用FWが設置されていた。攻撃者はこのリモート保守用FWの脆弱性を突いて給食事業者のシステムに侵入し、閉域接続を過信しておりパスワード・アカウント設定等のセキュリティ対策が甘かったため、閉域網を通して病院のシステムまでランサムウェアを感染させた。	• セキュリティポリシーの整備によるパスワードの複雑化 • ベンダーと病院間での責任分界点を明確化し、脆弱性を残さない運用を整備	参考資料③
5	自治体向けシステムへのマルウェア感染	• 2022年ＮＴＴデータ関西が自治体等向けに提供している電子申請サービスに付随するヘルプデスク業務で使用しているPCにマルウェアが感染した。 • マルウェアに感染したPCに保存されていた過去に送受信したメールが流出し、ヘルプデスクを装った攻撃者からの不審なメールが発信された。	• 社員への再発防止研修の実施 • 情報セキュリティ対策の強化	参考資料⑩

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料③ 病院を襲ったランサムウエア攻撃の報告書が公開
  病院を襲ったランサムウエア攻撃の報告書が公開 (nikkeibp.co.jp)
- 参考資料⑩ 不審メール（なりすましメール） に関するお詫びと注意喚起について
  （お知らせ）不審メール（なりすましメール） に関するお詫びと注意喚起について | ニュースリリース・お知らせ | 株式会社ＮＴＴデータ関西 (nttdata-kansai.co.jp)

セキュリティインシデント事例 – マルウェア感染 –（3/3）

参考資料1

マルウェア感染の発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
6	三和倉庫における不正アクセス	• 2022年、三和倉庫のサーバがランサムウェアの攻撃を受け停止した。 • 攻撃者はVPN 機器の脆弱性を突いた攻撃によりネットワーク内部に侵入し、ドメインコントローラから認証情報を取得、複数のサーバから機密情報を盗み出し、同時にランサムウェアを実行した。	• 脆弱性への対策とアカウント棚卸を行い、**多要素認証を徹底** • ネットワークセグメントの構成を見直し、内部FWを設置 • **EDR、SOCの導入** • 内部から外部への不審な通信をブロックするURLフィルタリングを導入	参考資料④
7	カプコンにおける不正アクセス	• 2020年、カプコンのネットワーク上の機器がランサムウェアの攻撃を受け暗号化された。 • 攻撃者はカプコン北米法人の予備の旧型VPN装置から不正侵入し、機器から情報を窃取した。その後、機器にランサムウェアを感染させ、各機器内のファイルを暗号化した。	• **SOCサービスを導入**し、外部との接続を常時監視 • 不正な挙動およびコンピュータウイルス感染の早期検知のため、最新の**EDRを導入** • インシデント発生時の迅速な対処に向け、ログの長期保存などの管理方法を改善	参考資料⑤

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料④ 不正アクセスに関する調査結果のご報告
  35-0.pdf (sanwasoko.co.jp)
- 参考資料⑤ 不正アクセスに関する調査結果のご報告
  不正アクセスに関する調査結果のご報告【第4報】| プレスリリース | 株式会社カプコン (capcom.co.jp)

セキュリティインシデント事例 – 誤操作・設定不備 –

参考資料1

誤操作・設定不備によるセキュリティインシデントの発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
1	福岡県における個人情報漏洩	• 福岡県の新型コロナウイルス感染症対策本部では、円滑な入院調整を行うため、必要な個人情報をクラウドに保存していたが、このクラウドへのアクセス権を付与したメールを1名に誤送信した。発覚後、ただちに誤送信先のアクセス権の削除を行ったが、削除処理が十分ではなく、誤送信先が個別のファイルを閲覧できる状態であった。	• 県以外の者に個人情報を提供する場合には、個人情報保護条例の規定に基づき、提供する個人情報の安全を確保するための必要な措置を実施 • だれが、いつ、情報にアクセスし、どのような処理を行ったか確認できるなど、セキュリティの高いファイル共有サービスを活用	参考資料⑨
2	トヨタ自動車におけるクラウド環境の誤設定	• 2023年4月、トヨタ自動車株式会社が、トヨタコネクティッド株式会社に管理を委託するデータの一部が、クラウド環境の誤設定により、公開状態となっていたことが判明した。 • 公開状態となっていた期間は2013年11月6日～2023年4月17日に及んだ。 • 外部より閲覧された可能性がある情報には、顧客約215万人の車載端末ID、車台番号、車両の位置情報、時刻が含まれていた。	• 従業員へのデータ取扱いのルール説明・徹底 • **クラウド設定を監査するシステムを導入** • **継続的にクラウド設定状況を監視する仕組みを構築**	参考資料⑪
3	JTBにおける情報共有ツールのアクセス権限誤設定	• 観光庁事業に補助事業者として関与しているJTBは、観光庁や間接補助事業者との情報共有を目的としてクラウドサービスを管理・運用していたが、当該クラウドサービスへのアクセス権限を誤設定したことにより、一部の間接補助事業者へ公開していない情報がダウンロードされた。 • 間接補助事業者にダウンロードされた情報には、当該事業の申請事業者及び申請事業者の連携先の個人情報を含む申請書類(最大11,483 人分の個人情報を含む1,698 件)並びに補助金交付申請書等が含まれていた。	• アクセス権限設定のチェック体制ならびに事業管理体制の徹底強化	参考資料⑫

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料⑨ 新型コロナウイルス感染症対策本部（調整本部）における個人情報の漏えい事案について
  新型コロナウイルス感染症対策本部（調整本部）における個人情報の漏えい事案について - 福岡県庁ホームページ (fukuoka.lg.jp)
- 参考資料⑪ クラウド環境の誤設定によるお客様情報の漏洩可能性に関するお詫びとお知らせについて
  クラウド環境の誤設定によるお客様情報の漏洩可能性に関するお詫びとお知らせについて | コーポレート | グローバルニュースルーム | トヨタ自動車株式会社 公式企業サイト (global.toyota)
- 参考資料⑫ 株式会社 JTB が管理・運用する情報共有ツールにおけるアクセス権限の誤設定による個人情報等の漏洩について
  情報漏洩に関するお詫びとお知らせ_221025.pdf (jtbcorp.jp)

セキュリティインシデント事例 – 紛失・盗難 –（1/2）

参考資料1

紛失・盗難の発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
1	兵庫県尼崎市におけるUSB紛失	• 兵庫県尼崎市は2022年6月、市の臨時給付金支給事業を受託した業者の関係者が、全市民約46万人等の情報が記録されたUSBメモリをカバンに入れて外部に持ち出した後飲食店に立ち寄り、飲酒し酩酊している間にカバンごと紛失した。 • 紛失したUSBメモリにはパスワードが設定されていたが、過去から市と委託事業者の間で使用されているものだった。 • 紛失したUSBメモリは後に発見されたが、格納された市民情報にはログインされた形跡が無く、このUSBメモリからの漏洩は認められなかった。 • 尼崎市は受託業者に委託者である尼崎市役所以外の事業所での作業許可を与えていたが、具体的な持ち出し方法についての指示や市の規程上必要とされるセキュリティ基準を遵守せず、業者に任せきりにしていた。	• 作業内容を事前に確認し、立会い有無や作業で取り扱う情報レベルを事前に確認する運用を徹底。 • サーバールーム等の情報ファイルを管理する場所での入退室管理を実施。遠隔接続・遠隔操作については記録をとり、外部電磁的記録媒体やPC等の持ち込みを規制。また、監視カメラ等の拡充も実施	参考資料⑬
2	愛知県豊橋市におけるUSB紛失	• 愛知県豊橋市は2020年5月、公営企業会計システムのデータを格納したUSBメモリを紛失した。 • 豊橋市では大規模災害時等におけるセキュリティ確保のため、バックアップデータを格納した媒体の外部保管を業者に委託しているが、当該システムの所管課である上下水道局総務課と情報企画課との媒体授受の過程においてUSBメモリを紛失したと考えられている。 • 紛失したUSBメモリには、上下水道局の公営企業会計システムのうち、債権者などの相手方情報が記録されていた。 • 紛失したUSBメモリに記録された情報には、開封時のパスワード要求や、閲覧にはシステム保守業者が解凍し公営企業会計システムを使用する必要がある等の保護がなされており、このUSBメモリからの個人情報の漏洩による被害等の情報は確認されていない。	• 情報企画課による業者保管用収納ボックスの入出庫の際の媒体確認の徹底 • 情報企画課と関係課間の媒体授受の双方による確認の徹底 • 通常時及び更新時における媒体の取扱いマニュアルの整備	参考資料⑭

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料⑬ 尼崎市 USB メモリ―紛失事案に関する調査報告書 houkokusyo.pdf (city.amagasaki.hyogo.jp)
- 参考資料⑭ 公営企業会計システム用バックアップUSBの紛失について 公営企業会計システム用バックアップUSBの紛失について/豊橋市 (toyohashi.lg.jp)

セキュリティインシデント事例 – 紛失・盗難 –（2/2）

参考資料1

紛失・盗難の発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
3	茨城県稲敷市におけるタブレット紛失	• 茨城県稲敷市は2019年8月、水道情報を記録した携帯型タブレット端末１台を紛失していた事を確認した。 • 紛失したタブレットに記載されていた情報には、10,801件分の加入者名、「水量メーター器」場所のほか、114件分の電話番号が含まれていた。 • 紛失したタブレットにはパスワードが施されており、2019年8月26日時点では、情報が第三者に利用された事実は確認されていない。	• 情報管理の徹底、職員のセキュリティ意識向上のための取り組みを実施	参考資料⑮

※対象資料の再発防止策より一部抜粋

【参考資料】

• 参考資料⑮ 水道情報を記録した携帯型タブレット端末の紛失について
水道情報を記録した携帯型タブレット端末の紛失について | 稲敷市公式ホームページ (inashiki.lg.jp)

セキュリティインシデント事例 – 業務外利用・不正持出 –

参考資料1

業務外利用・不正持出の発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
1	大阪府堺市の選挙データ流出	• 2015年、大阪府堺市の職員が作成したと思われる文書やマニュアルなどが、インターネット上で閲覧可能な状態にあることが発覚した。 • 市職員は有権者情報などのデータを市の選挙システムから持ち出し、個人契約の民間レンタルサーバーに保存していた。 • 2011年11月に開催された大阪府知事選挙時の、約68万人の有権者データを含むファイルが外部サイトからアクセスされ、個人情報が流出した可能性があるとされる。	• 既に実施している情報セキュリティに関するeラーニングについてレポート提出等を実施し、職員の意識向上効果を確認 • データのシステム外への持出し承認の二重化、持出しデータの暗号化、持出し操作ログ取得を拡充する仕組みを導入 • 情報セキュリティに関する統一的な窓口であるCSIRTを設置 • 自作システムについてデータの適正管理を徹底し、マニュアルを作成 • **ID、パスワード、アクセス権限の管理**を適切に実施	参考資料⑯
2	宮城県釜石市における市民の個人情報流出	• 2021年、宮城県釜石市の職員3名が市民の個人情報を不正に持ち出し、自宅パソコンのメールアドレスに送信し、保管していたことが判明した。また、同職員は不正に持ち出した市民情報を他部署職員に送信することで漏えいしていた。 • 持ち出された個人情報には、市民約３万２千人分の住基情報、624人分のマイナンバー等が含まれていた。	• 全職員を対象に情報セキュリティ研修を実施 • 情報資産に対し、機密性に応じた分類表示を徹底 • インターネットと遮断されたネットワークへ新たにパソコンを配置し、**三層分離を徹底** • 外部記録媒体への複写が可能な端末を限定 • インターネット接続系ネットワークで取り扱う電子ファイルの常時暗号化を施し、上長承認を経ないで外部に持ち出した電子ファイルは、内容を閲覧できない仕組みを導入	参考資料⑰
3	神奈川県真鶴町長による選挙人名簿不正利用	• 神奈川県真鶴町の現町長は、自身が立候補を予定していた町長選挙で利用するため，文書保管庫に収納されている使用済みの選挙人名簿をコピーし持ち出した。 • 現町長は、自身の選挙に際し、選挙人に選挙用はがきを郵送する際の宛名書きのため、当該名簿を利用した。	• 文書保管庫の入退管理を徹底 • **職員全員へIDを交付し、端末へのログイン・アウト管理**を徹底 • 文書の複写・持出し・庁舎外利用・私宅保管等厳禁の徹底化 • 職員に対する公式スマートフォン等の貸与による事務執行を導入し、デジタル化を推進	参考資料⑱

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料⑯ 堺市個人情報流出事案検証委員会報告書
  honpen.pdf (sakai.lg.jp)
- 参考資料⑰ 釜石市個人情報漏えい調査委員会報告書
  20272_.pdf (city.kamaishi.iwate.jp)
- 参考資料⑱ 選挙人名簿等流出に係る第三者委員会
  daisansyahoukoku.pdf (manazuru.kanagawa.jp)

セキュリティインシデント事例－メール誤送信－

参考資料1

メール誤送信の発生事例をWebで調査し、以下に取り纏めた。事例の詳細は参考資料を参照。

No.	事例名	インシデント概要	今後の対策など（※）	対象資料
1	福岡県職員によるメール誤送信	• 人間ドックを受診する福岡県職員等4,884名分個人情報を添付した電子メールを外部の医療機関に誤送信した。	• 受託業者における業務手順の適正化や個人情報の保護に係る研修の強化、作成終了データの複数人での内容確認を徹底。 • 総務事務厚生課においても当該事案を課内で周知するとともに、外部へメールを送信する際は複数人での最終確認を行うなどダブルチェックの指導・徹底	参考資料⑲
2	大阪府委託先事業者によるメール誤送信	• 2023年9月、大阪府商工労働総務課において実施する事業を請け負う委託事業者が、セミナーの案内を申込者2,056名にメールで送信した際、受信者本人とは異なる氏名をメールのあて先に記載していた。	• 事業者に対し、メールを送信する際には、送信先と送信内容に誤りがないか複数人の職員での確認を徹底するよう指導するとともに、個人情報を適正に取り扱うよう注意喚起を実施 • 所属内の職員に対して、本事案を周知し、改めて個人情報を適正に取り扱うよう、注意喚起を実施	参考資料⑳
3	東京都町田市におけるメール誤送信	• 2023年4月、町田氏は市外の幼稚園に対し、補助金等に係るデータをメールにて送信したところ、誤って他園に在籍する児童の情報を含むデータ（1,939 名分）を併せて送信した。	• データの管理を徹底するとともに、メール作成時及び送付時に、適切なデータが添付されているかを確認するよう、周知徹底。	参考資料㉑

※対象資料の再発防止策より一部抜粋

【参考資料】

- 参考資料⑲ 福岡県 県職員等の人間ドック受診者情報のデータの誤送信について
  県職員等の人間ドック受診者情報のデータの誤送信について - 福岡県庁ホームページ (fukuoka.lg.jp)
- 参考資料⑳ 個人情報が記載されたメールの誤送信について
  大阪府／報道発表資料／個人情報が記載されたメールの誤送信について (osaka.lg.jp)
- 参考資料㉑ 個人情報の漏えいについて
  20230417.pdf (city.machida.tokyo.jp)