2022年度 ITインフラ研究会
分科会A 活動報告資料

1. ガイドラインのマッピング

2.どうしたらいい？企業内セキュリティの在り方

2023年4月

ITインフラ研究会 分科会A

研究テーマ1

1. ガイドラインのマッピング

アジェンダ

①テーマ選定理由

②資料の使い方、見方について

①テーマ選定理由

■メンバーが抱えている課題を出し合う中で下記のような話があった

業務停止するようなインシデントもないし、BCPを作ろうとしてイメージ湧かない…

国・機関が出しているガイドラインを参考にしたらどうですか？

どんなガイドラインが存在するのかもわからない…
数多すぎて対象となるガイドラインがどれかの判別がつかない…

①テーマ選定理由

存在するガイドラインを一覧で網羅できて使い道がわかる資料があればなぁ～

①テーマ選定理由

■課題を出し合い大テーマとしてセキュリティを扱うとなった時

エンドユーザへのセキュリティ意識改革するには、どうしたら良いか…
自社のシステムによってセキュリティレベルがバラバラ…

システムについては要件・設計の段階で、どうするか決めておくのと
エンドユーザに対しては、ルールを作って意識させていくしかないのでは？

ルール作りってなかなかシステムと違ってインターネットや書籍にもナレッジなくて
0から作るのは難しくないですか？

①テーマ選定理由

0からセキュリティルールを作る時に参考になる資料がわかればなぁ～

①テーマ選定理由

という訳で

①テーマ選定理由

■各所に散らばっているガイドライン取りまとめた一覧表を作成した

※2023年3月時点のものであり、その後変更される可能性もあります

セキュリティの理解に役立つ(であろう)世の中のガイドライン

No	ガイドライン名	URL	業界	フェーズ	ガイド	想定読者	発行年	発行者
1	セキュリティの柱 - AWS Well-Architected Framework	https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/security-pillar/welcome.html	問わず	構築・設計	ベストプラクティス	開発者	適宜改定	Amazon Web Services
2	中小企業の情報セキュリティ対策ガイドライン　第3版	https://www.ipa.go.jp/security/keihatsu/sme/guideline/	問わず	企画	指針・手順や手法	経営者	2019年	独立行政法人情報処理推進機構
3	デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://cio.go.jp/guides	政府	全て	手順や各組織の役割等・政府共通ルール	PMO・システムオーナ	2019年	内閣官房　情報通信技術(IT)総合戦略室
4	システム構築の上流工程強化(非機能要求グレード2018)	https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html	問わず	要件定義・設計	非機能要求の確認	PMO・開発者	2018年	独立行政法人情報処理推進機構
5	地方公共団体における情報セキュリティポリシーに関するガイドライン	https://www.soumu.go.jp/main_content/000805453.pdf	すべて	企画・要件定義・設計	指針・手順や手法	発注者	2019年	総務省
6	IoTセキュリティガイドライン ver1.0概要(別紙2)	https://www.soumu.go.jp/main_content/000428394.pdf	すべて	企画・要件定義・設計	指針・手順や手法	発注者	2019年	総務省
7	クラウドサービス提供における情報セキュリティ対策ガイドライン(第3版)	https://www.soumu.go.jp/main_content/000771515.pdf	すべて	企画・要件定義・設計	指針・手順や手法	発注者	2021年	総務省
8	情報システムに係る政府調達におけるセキュリティ要件策定マニュアル	https://www.nisc.go.jp/policy/group/general/sbd_sakutei.html	官公庁	要件定義	RFPの策定にかかわる手順	発注者	2022年	内閣サイバーセキュリティセンター(NISC)
9	政府統一基準	https://www.nisc.go.jp/policy/group/general/kijun.html	官公庁	企画・要件定義	非システム系の方が要件を策定するための基準・ガイドライン	発注者	R3改定	内閣サイバーセキュリティセンター(NISC)
10	金融機関等コンピュータシステムの安全対策基準・解説書(第10版)	https://www.fisc.or.jp/publication/book/005409.php	金融	企画・要件定義・設計	設計の指針	金融機関のシステム企画部門	毎年改定	金融情報システムセンター(FISC)
11	PCI DSS v4.0	https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss	クレカ	設計・実装	設計・実装の指針	開発者	2022年	PCI SSC
12	サイバーセキュリティ経営ガイドライン Ver 3.0	https://www.meti.go.jp/policy/netsecurity/mng_guide.html	すべて	企画	体制構築	経営者	2022年	経済産業省/独立行政法人 情報処理推進機構

②資料の使い方、見方について

■表の各列の記載内容について

列名	説明
ガイドライン名	ガイドラインの名称
業界	一覧資料に記載しているガイドラインを発行している業界　官公庁・金融など
フェーズ	システム構築もしくは運用・保守の際に、ガイドラインを読むタイミング 例：企画・要件定義・設計・監査・啓蒙活動　など
ガイド	ガイドラインの記載内容を大まかを内容を記載しています。 例：指針・手順や手法・ベストプラクティス　など
想定読者	ガイドラインを読む際のターゲット読者 例：開発者・PMO・システムオーナー・エンドユーザ　など
発行年	発行年が古い場合、時代に適さない可能性があるため記載しています
発行者	ガイドラインを発行している機関・会社

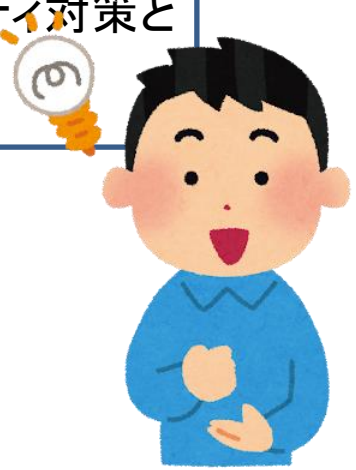
②資料の使い方、見方について

■注意点

- ■一覧資料は記載してあるガイドラインに**どんな時に参考にできるか**を記載した資料となります
- ■そのためガイドラインの内容を要約してまとめた資料ではないためご注意ください

ガイドライン「中小企業の情報セキュリティ対策ガイドライン」では、企業がセキュリティ対策を行なわないことで、発生するリスクとして金銭の損失・顧客の喪失・業務の停滞が発生

ガイドライン「中小企業の情報セキュリティ対策ガイドライン」は、
・中小企業の組織がセキュリティ対策の必要性を知りたい時
・担当者・従業員が具体的なセキュリティ対策として何をすれば良いかわからないときに参考になります。



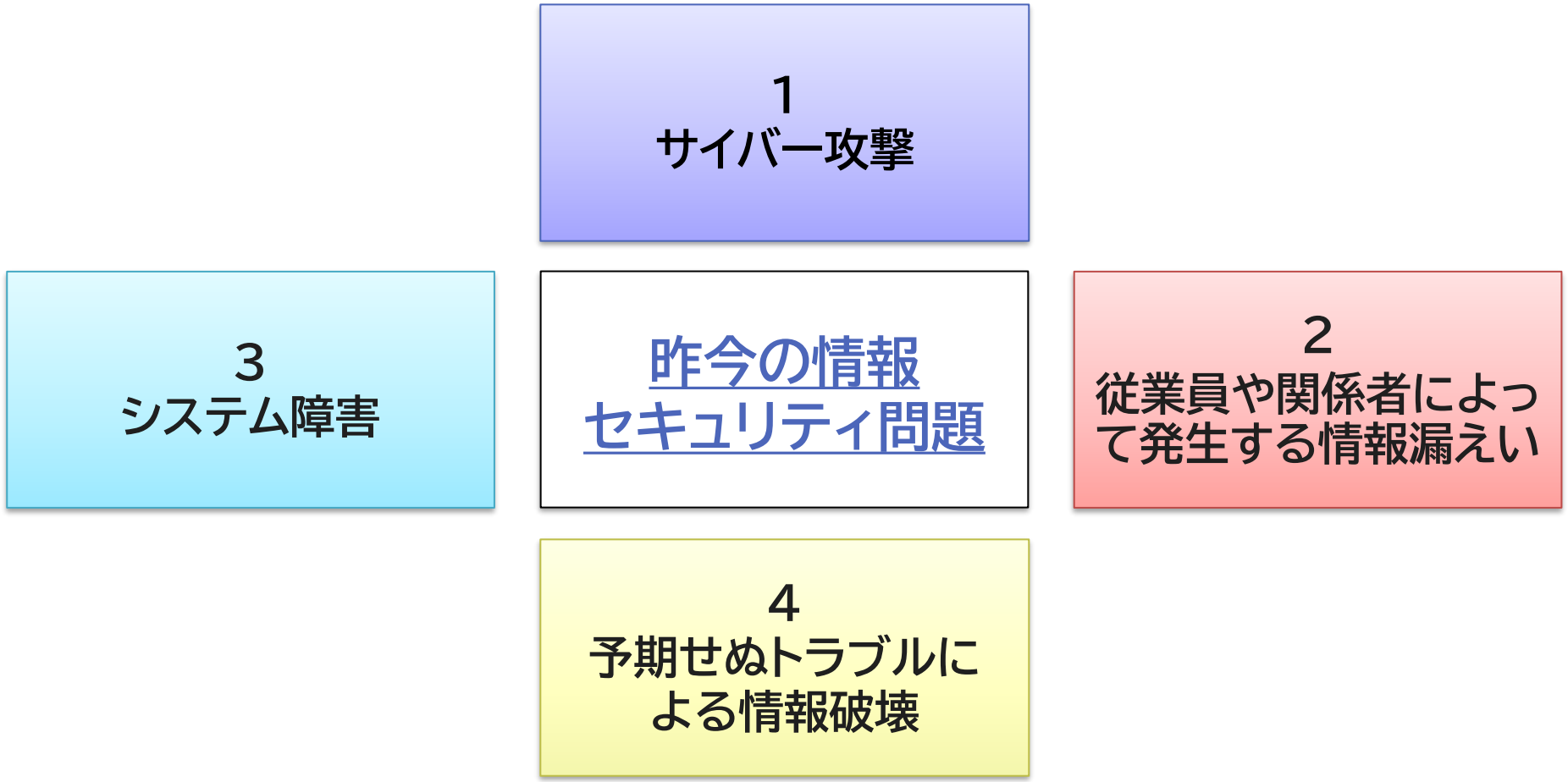
研究テーマ2

2. どうしたらいい？企業内セキュリティの在り方

情報セキュリティにおける主な4つの問題

情報セキュリティにおける主な4つの問題

以下に現在の主な情報セキュリティ問題を列挙すると共にJUAS内でのアンケート結果と照らし合わせ、
課題の洗い出し、および解決方法を述べていく。



情報セキュリティ問題を解決するには？

1 情報リテラシー教育の推進

悪意を持って情報漏えいをしてしまうわけではなく、

社員の情報リテラシーが低いがためにインシデントが発生してしまうケースがある。

そのため、従業員一人一人に、情報リテラシーを学んでもらうことは、過失による情報漏えいを防ぐことにつながる。

1 具体的な施策

- ✓ 定期的にセキュリティ教育を実施（上期2回、下期2回ずつ等、複数回開催するのが望ましい）
- ✓ インシデントが発生した事象をケースとしたビデオ視聴をし、影響範囲、および深刻度を体感・認識してもらう。
- ✓ ヒヤリハットを含めたインシデントケースのアンケートを実施後、内部で共有する。
- ✓ 職場で集会を開き、「どのように対応すればよいか」等ディスカッションを行う。

情報セキュリティ問題を解決するには？

2 セキュリティエンジニアの育成・確保

セキュリティエンジニアなどのサイバー攻撃を分析し、トラブル対応をする専門家を確保しておくことで、強固なセキュリティ対策が可能。社内のセキュリティ部門に高度な知識をもつ人材を配置することで、効率的・機能的なセキュリティ対策が実現しやすくなる。

2 具体的な施策

- ✓ **外部からセキュリティ人材を採用する。**
- ✓ **IT部の担当をセキュリティ専任として育成する。**
  （資格取得の奨励、積極的な教育の実施、およびセキュリティ専門の外部機関への出向）
- ✓ **現状の業務との兼任が殆どのケースだと思われるため、会社の協力のもと負荷を分散しながらセキュリティ分野へのスキル・経験を積んでいく必要がある。**

情報セキュリティ問題を解決するには？

3 情報管理ルールの徹底

情報セキュリティ向上のためには、リテラシー向上はもちろんだが、情報管理ルールを社内で徹底することが重要である。
誰がどのデータを管理しているのか、社外へ持ち出してはいけないデータはどれなのかなど、細かな点までルール化をする。
また、ルールを制定するだけではなく、責任者を決めることも必要。
責任者によってルールが適切に守られているかの管理が可能になり、徹底したセキュリティ対策が可能となる。

3 具体的な施策

- ✓ **セキュリティガイドラインの策定、および定期的な見直しの実施。**
- ✓ **セキュリティガイドラインの周知徹底　→定期的にテストを実施し、理解度を深める。**
- ✓ **責任者を選任し、管理権限を付与する。責任者が責任をもってセキュリティガイドラインを管理・運用をする。**

情報セキュリティ問題を解決するには？

4 統合的に管理できるセキュリティシステムの運用

セキュリティ対策には、複数のセキュリティを組み合わせる「多層防御」の観点も必要。個別に導入したウイルス対策ソフトやファイヤウォールでは、脅威がすり抜けてしまう可能性がある。
そのため、自社で利用しているさまざまなシステムを、統合的に管理できるセキュリティシステムの運用が有効である。
また、セキュリティシステムが一つではなく複数ある場合には、それぞれの管理をしないといけないため、コストや人材が必要となる。それらを統合的に管理できるセキュリティシステムを選ぶことで、運用コストや人材コスト面から見ても効率的であるといえる。

4 具体的な施策

- ✓ FWだけでなく、IPS/IDS、およびWAFを導入することで多層防御を可能とする。
- ✓ 社内だけでなく社外（在宅勤務等）からもセキュアな通信が可能となるよう、エンドポイントセキュリティの強化、およびクラウドPROXYを採用する。
- ✓ ただしコスト増となってしまうため、予算とのバランスを考慮し、優先度の高いものから実施していく。