資料３

地方公共団体の情報セキュリティ対策に係る検討事項

総務省

2022年８月30日

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の改定等に係る検討会

最近の地方公共団体における情報セキュリティインシデントについて①

① 委託先事業者に関連した情報漏えい

インシデント事例

○概要

令和4年6月に委託先会社の再々委託先の社員が全市民情報が入ったUSBメモリーを紛失した。

○主な原因

・委託先会社が外部へのデータ持出しにおける具体的な運搬方法等について市の許可を得ていなかったこと
・作業終了後に速やかにデータを削除せず、個人情報を所持したまま飲食店に立ち寄ったこと
・委託先への十分なセキュリティ対策の確認・徹底不足

○課題

委託先のセキュリティ対策管理の徹底

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

第３編　第2章　情報セキュリティ対策基準（解説）

1～2（略）

3.情報システム全体の強靭性の向上

4～7（略）

8.業務委託と外部サービスの利用

8.1.業務委託

9～10（略）

委託先の情報セキュリティ対策の管理、委託先への要求事項を調達仕様書等に定めることに関する記載（iii-38）

委託先の責任範囲の明確化、委託を行う際の情報セキュリティ要件、再委託の留意点等に関する記載（iii-132～136）

最近の地方公共団体における情報セキュリティインシデントについて①

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

8　業務委託と外部サービスの利用
8.1　業務委託　【例文】
(1)　(略)
(2)　契約項目
情報システムの運用、保守等を業務委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。
・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

(3)　確認・措置等
情報セキュリティ管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(2)の契約に基づき措置を実施しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

最近の地方公共団体における情報セキュリティインシデントについて①

地方公共団体における調達・運用時の情報セキュリティ対策の実施状況

〇委託先管理について、調達時におけるセキュリティポリシーに基づいた要件の記載や契約等で情報漏えい防止策を義務付けている団体は多いが、運用時における管理が不十分な実態がある。

	都道府県	割合	市区町村	割合
情報資産の調達の際、仕様書等に情報セキュリティポリシーに基づいた要件を記載している	47団体	100%	1406	80.8%
委託事業者に対し、情報漏えい防止策を契約等により義務付けている	47団体	100%	1705	97.9%
情報システムの運用等の委託事業者に対する指導・監査を実施している	34団体	72.3%	1033	59.3%
機密性、完全性、可用性等についてサービス規約(SLA)に定め、委託業者に対し定期的に報告することを定めている	30団体	63.8%	868	49.9%

（参考：総務省「令和3年度 自治体DX・情報化推進概要」）

対応の方向性

➢ ガイドラインには、すでに委託先の管理の徹底等について記載されているが、特に運用面における管理が十分でない実態がある。このため、ガイドラインに記載を新たに追加するのではなく、委託先の管理に関する確認項目等について定期的な注意喚起を実施し、対策の徹底を求めていくことが重要ではないか。

最近の地方公共団体における情報セキュリティインシデントについて②

② ランサムウェアの感染

インシデント事例

○概要

令和３年１０月に病院の端末がランサムウェアに感染。電子カルテシステムなどのシステムが停止し、緊急・新規患者の受け入れが停止した。

※病院については、所管である厚生労働省策定の「医療情報システムの安全管理に関するガイドライン」に基づいてセキュリティ対策が実施されており、本事案の対応についても、厚生労働省が行っている。

○主な原因

- セキュリティを考慮したシステムの構築・運用を実施していなかったこと
- インターネット接続機器等の脆弱性の放置、アップデートの未適用、サポート終了OSを利用していたこと
- ウィルス対策ソフトを停止してシステムを利用していたこと

○課題

病院、サポートベンダ両者の適切なセキュリティ対策を行っていなかったこと

（参考）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

第2章　情報セキュリティ対策基準（解説）

1～2（略）

3.情報システム全体の強靭性の向上

4～5（略）

6.技術的セキュリティ

7～8（略）

9.評価・見直し

10.用語の定義

- 機器に関する脆弱性の有無の確認、脆弱性が存在する場合のパッチ適用やバージョンアップの実施に関する記載（iii-84）
- Webアプリケーションにおける脆弱性対策の参照先の記載（iii-105）
- 計画的な脆弱性対策の実施・検証・緩和策の実施に関する記載
  サポート終了OSによる脆弱性リスクに関する記載（iii-117-119）
- 技術的な脆弱性の悪用に対する点検について参照先の記述（iii-160）

最近の地方公共団体における情報セキュリティインシデントについて②

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

６．技術的セキュリティ
６．６ セキュリティ情報の収集
（１） セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等
セキュリティホールは日々発見される性質のものであることから、積極的に情報収集及び対応の検討を行う必要がある。セキュリティホールの対策状況の定期的な確認により、セキュリティホールへの対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連するセキュリティホールの情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関するセキュリティホールへの対策計画を策定し、措置を講ずることが必要である。
（注１）セキュリティホールの情報収集に関しては、情報収集の体制、分析の手順、情報収集先、情報共有先等を決めておくことが望まれる。
（注２）セキュリティホールの緊急度のレベルに応じて、更新の実施の有無を検討する。深刻なセキュリティホールが発見された場合は、直ちに対応しなければならないが公開された脆弱性の情報がない段階においては、サーバ、端末及び通信回線上で取り得る対策を検討する。また、更新計画を定め、他のシステムへの影響、テスト方法、バックアップの実施、パッチの適用後のシステム障害が生じた場合の復旧手順等を盛り込むことが望ましい。
　なお、近年のIT の利活用拡大により、システムで使用しているソフトウェア等の種類も増加していることから、IT 資産を手作業で漏れなく正確に把握するには多大な労力が必要となる。そのため、自動でソフトウェアの種類及びバージョンを管理する機能を有するIT 資産管理ソフトウェアを導入することが考えられる。また、脆弱性対策が計画通りに実施されないことは、システムの損傷、情報漏えい等の情報セキュリティインシデントが発生する原因にもなるため、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認することが望ましい。

対応の方向性

- 脆弱性が放置されていれば、サイバー攻撃のリスクが高まるため、適切なセキュリティ対策と構成管理による漏れの無いパッチ適用が重要となる。ガイドラインには、脆弱管理の必要性とその脆弱性によるリスクについて記載されており、また、ＮＩＳＣ、Ｊ－ＬＩＳ等の関係機関とも連携し、地方公共団体への脆弱性情報等の情報共有を行っているところである。その上で、地方公共団体の職員が共有された情報を基に具体的に対応を行うようにする方策を検討するなど、実効性を高めていくことが重要ではないか。

最近の地方公共団体における情報セキュリティインシデントについて③

③ マルウェア「Emotet」の感染再拡大

Ｅｍｏｔｅｔについて

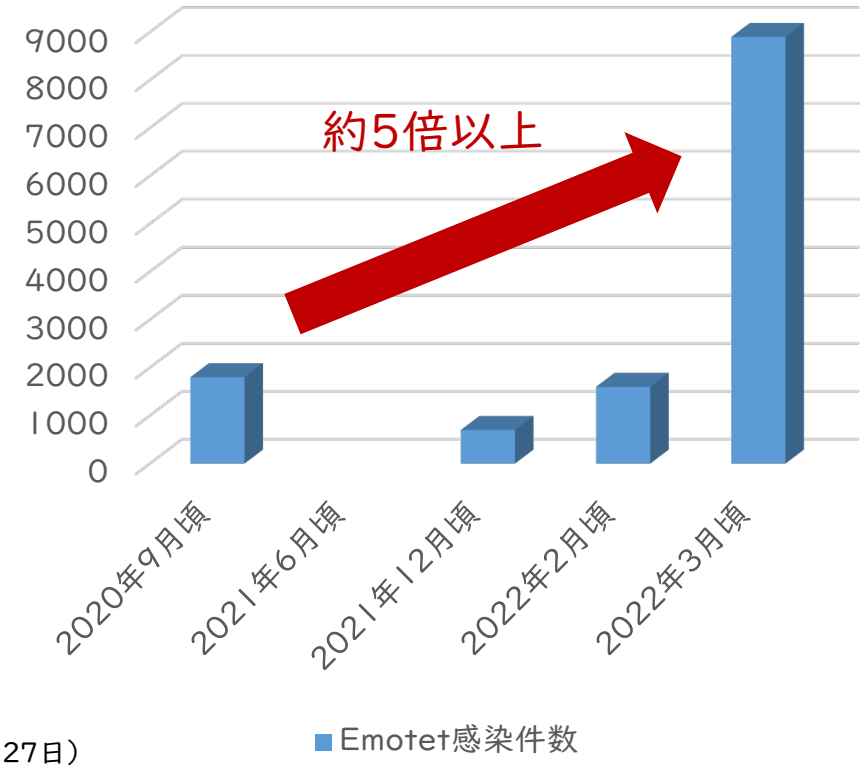
○概要

Emotetは、悪意のある攻撃者によって送られる不正なメールから感染が拡大しているマルウェア。

令和４年３月に入り、Emotet感染件数が令和２年の感染ピーク時の約５倍以上に急増している。

○特徴

・メールの添付ファイル（ExcelやWord）やこれらを含むパスワード付ZIPファイルの実行で感染
・メール本文中のリンクをクリックすることで感染
・なりすまし元の組織名や署名などが記載されるケースも存在



（参考）JPCERTCC,マルウェアEmotetの感染再拡大に関する注意喚起,令和4年5月27日）
https://www.jpcert.or.jp/at/2022/at220006.html

最近の地方公共団体における情報セキュリティインシデントについて③

インシデント事例

〇被害を防いだ事例
- ・不審ファイルを開いたが、セキュティクラウドによる検知が行われた。
- ・メール・ファイルの無害化によって直接的な被害を防ぐことができた。

〇確認・報告が遅れた事例
- ・不審ファイルを開いたが、本人からの報告が無かった。
- ・Emotet検査ツール等を使用したが検出できなかったため対応を行わなかった。

対応の方向性

- ➢ 「不審な添付ファイルは開かない」、「感染が疑われる場合の報告」等の組織内での一般職員向けの研修や注意喚起を行うとともに、地方公共団体の職員が研修や注意喚起を踏まえ、具体的に対応を行うようにする方策を検討していくことが重要ではないか。
- ➢ 世界的な脅威となっているランサムウェア、Emotet、フィッシングメール等への対応に関しては、ガイドラインにマルウェアの特徴、留意点、対策等について追記を行う。