IPA news

vol.55
1月号

「IPA NEWS」はIPAの日々の活動をわかりやすくご紹介する広報誌です。

特集

中小企業も他人事ではない!?

“制御システム”のセキュリティ対策

- データで読むITの今・未来
  社会インフラに甚大な影響！ 脅威に備えた対策を
- セキュリティのすゝめ 04〈クラウドサービスを利用する際の留意点〉
  利用者も責任を果たして安全なクラウドサービスを
- IPAの最新情報をまとめてお届け！
  Hot & New Topics
- 目指せ！ 情報処理のエキスパート!!
  国家試験に挑戦！ ～ITパスポート試験編～

中小企業も他人事ではない!?

“制御システム”のセキュリティ対策

▶左から
北海道電力株式会社 情報通信部
情報セキュリティ統括グループ 主任
村上 幸司さん

中部電力パワーグリッド株式会社
本社 システム部
総括グループ 副長
長谷川 弘幸さん

IPA
産業サイバーセキュリティセンター
事業推進部 事業推進グループ
グループリーダー **中山 顕さん**

凸版印刷株式会社
情報セキュリティ本部
セキュリティ推進部
監理チーム 係長 **坂田 尚さん**

社会インフラや産業基盤を支える「制御システム」への攻撃が増えています。企業のセキュリティ戦略を牽引する人材を育てるIPAの「中核人材育成プログラム」の担当者と、このプログラムの修了者3名に、制御システムのセキュリティを取り巻く実態や社会インフラ業界のサプライチェーンに関わる中小企業が取るべき対策などを聞きました。

社会インフラなどに影響を及ぼす脅威とは

電力やガス、化学、鉄道業界といった社会インフラや産業基盤を支える組織の「制御システム（OT／Operational Technology）」を狙ったサイバー攻撃が世界各地で拡大傾向にあります。「日本も無縁ではありません。すでに攻撃されているかもしれないと考え、特に中小企業の皆さんには早急な対策を講じてほしいと思います。対策が手薄な企業が攻撃の“踏み台”となり、サプライチェーン全体や取引先の大手インフラ企業の操業に危害を及ぼすこともあるからです」とIPA産業サイバーセキュリティセンターのグループリーダー・中山顕さん。中山さんは、セキュリティの観点から経営層と現場担当者をつなぐ人材を育てる「中核人材育成プログラム」の運営も担当しています。

「サイバー攻撃への備えを早急に」と語るIPAの中山さん

同プログラム修了者の長谷川弘幸さん（中部電力パワーグリッド）によると、最近ことに目立つのはランサムウェアの被害だそうです。「ベンダー調査※によると、2021年上半期にこの影響を受けた組織数は前年同期で約2倍に上ります」とのこと。ランサムウェアは、業務システムなどに代表される情報システム（IT／InformationTechnology）の被害が多いのですが、業務に関連するOTや社会インフラを支えるOTが影響を受けることもあるといいます。

坂田尚さん（凸版印刷）によれば、一般的に重視する要素を順に挙げると、ITは「機密性→完全性→可用性」、OTは「可用性→完全性→機密性」と異なるとか。また、IT系は新技術をすぐに取り入れるのに対し、OT系は十分に検証した技術のみを採用するといったように、常に安定稼働が優先されますが、昨今ではサイバー攻撃による操業停止などのリスクが懸念されています。

村上幸司さん（北海道電力）は、自社OTのセキュリティ業務のほか、中核人材育成プログラム修了者コミュニティ「叶会」で中小企業のセキュリティ向上に取り組んでいます。「サプライチェーン全体のセキュリティの底上げは、インフラを管理・運用する当社のような企業にとってリスク対策の一環。発注元企業は、中小企業が攻撃の“踏み台”となることへの危機感を持つ必要があります」と村上さん。

社会インフラの業界以外でも、サプライチェーンのまとめ役となる大手企業がデータの取り扱いについてセキュリティ基準を設けるなどの対策が進んでいます。坂田さんは「印刷データのやりとりには多くの中小企業や個人事業主が関与します。当社では個人情報の取り扱いをはじめ、使用する外部記憶媒体の種類、使用済みデータの廃棄法など、セキュリティ基準を満たした事業者とのみ業務委託する決まりで、これがサプライチェーン全体を守るひとつの手立てにもなっています」と明かします。

社会インフラやサプライチェーンを守るための具体策

「大手インフラ企業などを取引先に持つ中小企業の皆さんに実践していただきたいのが“踏み台”にならないためのITのセキュリティ対策。『OSやソフトウェアは常に最新の状態にする』『不審なメールの添付ファイルやURLは開かない』『情報管理のパスワードを強化する』などの基本的な対策が有効です。逆に、対策を怠ることで自社へのサイバー攻撃の被害が取引先にも及び、損害賠償を請求されるケースもあります」と中山さん。

これらに加えて長谷川さんは、「自社を知ろう、守ろう、戻そう」という3つのキーワードを挙げます。まずは、自分たちが守るべきものや自社のセキュリティレベルを「知る」こと。現状を的確に把握できていなければ適切な対策が打てません。現状把握にはIPAの「中小企業の情報セキュリティ対策ガイドライン」も役立ちます。「守る」という点では、中山さんが挙げる対策はもちろんのこと、「サイバーセキュリティお助け隊サービス」が中小企業にとっては安価で、しかも監視サービスもつくためお勧めとのこと。最後の「戻す」は、ランサムウェア攻撃を受けた場合を想定し、いつでもデータを戻せるようにしておくことです。「攻撃によっては単純にバックアップを取るだけでは戻せないケースもありますが、まずは自分たちにとって大事な情報を決め、日ごろからバックアップを取っておくとよいでしょう。戻せる状況をつくっておけば、万一の場合も事業を継続できる可能性が高まります」と長谷川さん。

村上さんは、「中小企業の情報セキュリティ対策ガイドライン」と合わせて、中小企業自らが情報セキュリティ対策に取り組むことを宣言する制度「SECURITY ACTION」の活用も推奨します。「現状分析から始めて自社の取り組み目標を決めることで、自社に合った実効性の高い対策を実践できます。さらに、意識を高めるための従業員教育や中小企業間の情報共有も課題となるでしょう」と指摘してくれました。

「事業に沿ったインシデント演習を定期的に実施すると、セキュリティの弱点をあぶり出せます」と語るのは坂田さん。セキュリティの専門家が社内にいない場合は、専門書を参考にしたり、外部のサービスを活用するのも一案です。

中山さんは中小企業の対策の普及はまだ十分でないと指摘したうえで、最後にこう語ります。「社会インフラを守るには、サプライチェーン全体で防御を固め、脅威は他人事でないと肝に銘じること、そしてリスクを認識することがなにより重要なのです」

※https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/

基本の対策に加え、「自社を知り、守り、戻す」を徹底！

中部電力パワーグリッドで送配電OTのセキュリティ戦略を担う長谷川さん

凸版印刷グループのセキュリティ対策に取り組む坂田さん

北海道電力グループ全体のセキュリティ対策に取り組む村上さん

データで読むITの今・未来

社会インフラに甚大な影響！脅威に備えた対策を

制御システム（OT）と情報システム（IT）の融合が進んでいることで、情報システムへのサイバー攻撃が、制御システムに深刻な影響を及ぼすケースなどが増えています。

〈参考資料〉「情報セキュリティ白書2021」
https://www.ipa.go.jp/files/000094186.pdf

制御システムのインシデント事例

発生国	発生年月	概要
日本	2020年6月	国内自動車メーカーの社内サーバーが攻撃され、同社のネットワークを介してウイルスが拡散。これによりシステム障害が生じ、国内外の生産拠点の一部の操業が停止した。特定の制御システムのプロセスを強制停止するように設計されているランサムウェア「Snake」（別名、EKANS）による攻撃と推測される。
米国	2020年2月	天然ガス圧縮施設の情報システムと制御システムのWindowsコンピュータがランサムウェア感染により停止。制御はPLCにより行われていたため制御不能になることはなかったが、制御信号がモニタできなくなり、2日間にわたり運用を停止した。攻撃者は、標的型メールにより情報システムに侵入し、制御システムへの攻撃へと展開した。
インド	2020年10月	ムンバイで大規模停電が発生。交通管理システムや列車の運行に大きな混乱をもたらし、インフラサービスの復旧に2時間を要した。電力会社や送電会社のサーバーへの複数の不正ログイン、電力網の運用を監視、配電管理を行う負荷分散センター内のウイルス感染などが確認されている。
米国	2021年2月	水道局の水処理システムへの不正アクセスによって、水処理に用いる水酸化ナトリウム投入量が一時的に通常の約100倍に設定された。異変に気付いた管理者がすぐ対応したため実害は免れた。当水道局では、2020年1月にサポートが終了したWindows7が浄水場のすべてのコンピュータで使用されており、リモートアクセス用には共有パスワードが使われていた。
米国	2021年5月	米国の燃料パイプライン最大手のColonial Pipelineが、サイバー攻撃によりランサムウェアに感染し、業務を停止した。この停止は6日間続き、米国東部南部でガソリンスタンドの休止や油価の上昇を招いた。本ケースではデータの暗号化だけでなくデータの窃取も行われ、100GB近いデータが窃取されたと報道されている。

増加する制御システムのセキュリティリスク

- Honeywell International, Inc.が調査した脅威のうち、産業用制御システムに大きな混乱を引き起こす可能性のあるUSBメモリを媒介とするウイルスの脅威

26%（2018年） ➡ **79%**（2020年）

「Honeywell Industrial Cybersecurity USB Threat Report 2021」より

- NCCICが公開した制御システムの脆弱性情報件数

192件（2018年） ➡ **224件**（2020年）

そのうち**77.7%（174件）**が遠隔から攻撃可能な脆弱性

業務用に持ち込んだUSBメモリやパソコンの接続、IIoT（Industrial Internet of Things）機器の導入、コロナ禍における遠隔アクセス等の利用拡大などによって制御システムが外部から攻撃を受けるリスクも高まっています。また、最近では、金銭目当てで企業・組織内のネットワークへ侵入し、パソコンやサーバー上のデータをランサムウェアにより一斉に暗号化して使用できなくする、データそのものを窃取して公開すると脅迫する、という「二重の脅迫」の手口も多く確認されるようになっています。

リスク感度を高め、リスクに応じた対策を実践することが重要です。

手軽に使えるからこそ対策はしっかりと！

利用者も責任を果たして安全なクラウドサービスを

❗利用企業は5年で約1.5倍に増加

インターネットを通じてアプリケーションやOS・ミドルウェア、ハードウェアなどを扱う「クラウドサービス」の利用が増えています。2016年に46.9％だった利用率は2020年に68.7％へと拡大（総務省「令和3年版情報通信白書」）。便利な情報システムを自社で所有せず安定的に使えるという手軽さがメリットです。

しかし、安易な利用はさまざまな問題を引き起こします。例えば、クラウドサービスの障害に伴う業務停止やサイバー攻撃による情報漏えいなど「サービス提供者側の問題」はそのひとつです。

また、「利用者側の問題」として多いのは安易なパスワード設定による不正ログイン被害です。なりすましや標的型攻撃のための情報収集に悪用されることがあります。このほか設定の不備による誤公開なども利用者側の問題です。

サーバーが設置されている国の法制度にシステムの運用が影響を受ける「法律上の問題」もあります。2022年4月に施行される改正個人情報保護法でも、情報を取り扱っている国の環境を理解し利用者に通知するという外的環境の把握が盛り込まれました。

❗“影のITシステム”から情報が漏えいすることも

「中小企業のためのクラウドサービス安全利用の手引き」では、「選択」「運用」「セキュリティ管理」というシーン別に15項目のチェックリストを設け、これらの問題を回避するための留意点を示しています。表はその抜粋です。

どの項目も重要ではあるものの、利用者がことに気をつけたいのは「運用」面です。従業員が私的に利用しているクラウドサービスを業務でも利用し、会社の知らない“影のITシステム（シャドーIT）”から情報が漏えいするケースもあるので、誰が使うか、どう管理するかの確認が必要です。IDは1人ずつ発行し、パスワードは推測されにくい複雑なものにするなど厳格に管理しましょう。

個人契約のクラウドサービスが業務に不可欠となっている場合は、そのサービスを会社で契約し直してサポート体制を整えます。それができない場合は、クラウド上では重要な情報をやりとりしないことを社内で徹底するようにしましょう。

「選択」にあたっては事業者やサービスの信頼性を提供実績や品質保証基準（SLA）などで確認する必要がありますが、その際は「政府情報システムのためのセキュリティ評価制度」（ISMAP）や民間団体のクラウド認証制度等も参考になります。

クラウドサービスは安定して稼働するうえ、基本のセキュリティもしっかりしていますが、利用者側のID・パスワード管理や公開範囲の設定がずさんでは足をすくわれます。サービス利用者と事業者の責任の範囲を認識し、それぞれが万全の対策を実施することでクラウドサービスのセキュリティは維持・向上できるのです。

クラウドサービス安全利用チェックシート（抜粋）

●選択するときの確認ポイント（6項目）
- ・何に使うか、どんな情報を扱うか？
- ・サービス事業者は信頼できるか？

●運用するときの確認ポイント（4項目）
- ・誰が使うか、どう管理するか？
- ・利用者認証は厳格にできているか？

●セキュリティ管理のポイント（5項目）
- ・事業者のセキュリティ対策は、サポートは？
- ・データ保存先はどこの地域か？

＋ 対策のポイント ＋

1. 自社の状況や外部の評価も交えて、扱う情報や利用するサービスを選ぶ。
2. 利用者側の責任を認識し、パスワードや設定に注意。従業員にもルールを徹底。
3. サーバーが置かれている国の環境など、法律上の問題も考慮する。

もっと詳しく知りたい方は… https://www.ipa.go.jp/files/000072150.pdf

「制御システム関連のサイバーインシデント事例」第8、9集を公開

本シリーズは、IPAの「制御システムのセキュリティリスク分析ガイド」で示すリスク分析の実践を支援する資料です。サイバー攻撃によって事業被害が発生するシナリオを想定し、攻撃の流れからリスクを評価する「事業被害ベースのリスク分析」の実践が可能になります。第8集では、2021年2月の米国水道局への不正侵入と飲料水汚染未遂の事例、第9集では、同5月の米国最大手パイプライン企業でのランサムウェア感染被害の事例を解説。本書を活用しながら攻撃の流れの可視化（攻撃ツリーの作成）やリスク評価を行うことによって、類似事例が発生した際の事業への影響の分析や、リスク低減に効果的な緩和策の特定などを行うことができます。

https://www.ipa.go.jp/security/controlsystem/incident.html
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

● **米国最大手のパイプライン企業でのランサムウェア感染被害の事例（攻撃ツリー）**

攻撃局面	攻撃ステップ項番	攻撃シナリオ / 攻撃ツリー・ステップ / 〈情報システムをランサムウェアにより暗号化することにより、制御システムの稼働を停止する。〉
【A1】	S1	侵入口＝VPN装置 VPNの正規のパスワードを利用し、組織内へ侵入する
【A2】	S2	業務端末Aから組織内ネットワークを探索し、機密情報を探し出すと同時に、攻撃範囲を広げる調査を行う
【A3】	S3	探し出した機密情報を、組織外部へと運び出す
【A4】	S4	攻撃対象とした組織内の情報ネットワークのコンピュータにランサムウェアを送り暗号化する
【A5】	S5	制御システムへのランサムウェアの被害拡大を防ぐため、現場担当者が制御システムをシャットダウンする

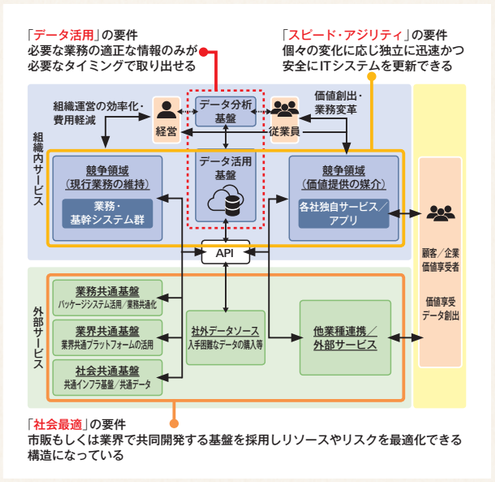
「DX実践手引書 ITシステム構築編」を公開

本書は、DX実現に向けたITシステムの構築を支援するガイドです。国内企業のDX先進事例の調査から得られた教訓をまとめたもので、DX戦略の考え方からITシステムのあるべき姿、それらに対する具体的な技術的アプローチなどを解説しています。また、DXの実現に向けてITシステムに求められる共通の要素（社会最適、データ活用、スピード・アジリティ）を明確化し、それらを社内のITシステムのどの要件の中で実現するかを技術要素群とともに図示した、ITシステムの全体像「スサノオ・フレームワーク」を提示しています。

これらの活用で、自社の現行システムの分類や、外部ITシステムとの協調・連携を前提にしたITシステムの刷新の検討などが可能になります。

https://www.ipa.go.jp/files/000094497.pdf

● **DX実現のためのあるべきITシステムの全体像「スサノオ・フレームワーク」**



DXポータルサイト「DX SQUARE」をオープン

「DX SQUARE」は、DX関連情報のポータルサイトです。国内企業のDX推進の支援を目的にしたもので、「DXを学んで、知って、実践する」をコンセプトに、DXの知識を深めたい方、DX推進に向けて具体的な戦略を検討したい方、すでにDXへの取り組みを始めている方などの、それぞれの層のニーズや目的に応じた情報を発信しています。

DXに取り組む企業へのインタビュー記事や用語集、解説映像、お役立ちツールといった各種コンテンツを取り揃えているため、DX推進の具体的なイメージをつかめていない方でも、DXの考え方を学び、理解を深めることができます。また、DXを進めるうえでのヒントや新たなアイディアのリサーチ、トレンドの把握といった目的でも有効に活用いただけます。

https://dx.ipa.go.jp/

● **DX関連情報のポータルサイト「DX SQUARE」**

Just Information

オンデマンド配信コンテンツのご紹介

IPAのYouTube公式チャンネル「IPA Channel」では、各種動画コンテンツを配信中。
新たに公開した2本のコンテンツをご紹介します。

IPAデジタルシンポジウム2021

2021年10月に開催した「IPAデジタルシンポジウム2021」のアーカイブ動画。「DXとセキュリティ対策の両立はどこまでやるべき？」「DX推進にどんな人材が求められる？」といったDXの課題について各界のスペシャリストと一緒に考えます。DXに取り組む企業の経営層、事業部門の皆さまにおすすめ。

▼**視聴はこちら**

デジタルシンポジウム　IPA　検索

https://www.ipa.go.jp/event/ipasympo2021.html

IPA中小企業情報セキュリティ講習能力養成セミナー

中小企業向けの情報セキュリティ講習会を行うためのハウツー動画。IPAの無償コンテンツを活用したプログラムの構成例や、説明のポイントなどを解説します。講師の実務経験がない方でも、講演に必要なノウハウを習得することができます。中小企業の教育担当者や、中小企業向けにセキュリティコンサルを行う方などにおすすめ。

▼**視聴申込みはこちら**（お申込みいただいた方に視聴URLをご案内します。）

講習能力養成セミナー IPA　検索

https://www.ipa.go.jp/security/keihatsu/sme/seminar.html

独立行政法人情報処理推進機構
〒113-6591 東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス

URL●https://www.ipa.go.jp/
掲載写真の一部は、Shutterstockのライセンス許諾により使用しています。

目指せ！ 情報処理のエキスパート!!

国家試験に挑戦！ ～ITパスポート試験編～

ITパスポート試験（iパス）は、IT社会で働くすべての社会人が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

問1　ストラテジ系【令和3年度・問30】

情報の取扱いに関する不適切な行為a～cのうち，不正アクセス禁止法で定められている禁止行為に該当するものだけを全て挙げたものはどれか。

a　オフィス内で拾った手帳に記載されていた他人の利用者IDとパスワードを無断で使って，自社のサーバにネットワークを介してログインし，格納されていた人事評価情報を閲覧した。
b　同僚が席を離れたときに，同僚のPCの画面に表示されていた，自分にはアクセスする権限のない人事評価情報を閲覧した。
c　部門の保管庫に保管されていた人事評価情報が入ったUSBメモリを上司に無断で持ち出し，自分のPCで人事評価情報を閲覧した。

ア　a　　**イ**　a，b　　**ウ**　a，b，c　　**エ**　a，c

問2　マネジメント系【令和2年度10月・問45】

ITガバナンスの説明として，最も適切なものはどれか。

ア　企業が競争優位性構築を目的に，IT戦略の策定・実行をコントロールし，あるべき方向へ導く組織能力のこと
イ　事業のニーズを満たす良質のITサービスを実施すること
ウ　情報システムにまつわるリスクに対するコントロールが，適切に整備，運用されていることを第三者が評価すること
エ　情報セキュリティを確保，維持するために，技術的，物理的，人的，組織的な視点からの対策を，経営層を中心とした体制で組織的に行うこと

問3　テクノロジ系【令和2年度10月・問99】

IoTデバイスとIoTサーバで構成され，IoTデバイスが計測した外気温をIoTサーバへ送り，IoTサーバからの指示でIoTデバイスに搭載されたモータが窓を開閉するシステムがある。このシステムにおけるアクチュエータの役割として，適切なものはどれか。

ア　IoTデバイスから送られてくる外気温のデータを受信する。
イ　IoTデバイスに対して窓の開閉指示を送信する。
ウ　外気温を電気信号に変換する。
エ　窓を開閉する。

正解：問1ア　問2ア　問3エ

IPAの事業領域

情報セキュリティ対策の実現
- サイバー攻撃の脅威から社会を守る
- セキュリティ対策を促す
- セキュリティを担保する

IT人材の育成
- サイバーセキュリティ人材を育てる
- ITイノベーション人材を育てる
- IT人材の知識・スキルを認定する

IT社会の動向調査・分析・基盤構築
- IT社会の動向を分析する
- スキル変革を促進する
- システムの安全性・信頼性を確保する
- 企業のDXを促進する
- 地域のIoTビジネスの創出を支援する
- 社会のアーキテクチャを設計する
- データの相互運用性を高める

「IPA NEWS」定期送付のお申込み、送付先の変更は、
下記のメールアドレスにご連絡くださいますようお願い致します。
メール　pr-inq@ipa.go.jp

IPAのSNS公式アカウント、メールニュースの配信登録はこちら
https://www.ipa.go.jp/

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan