特集

社会インフラシステムにおけるサイバーセキュリティ

―レジリエントで持続可能なデジタル経済社会に向けて―

編集にあたって

石黒正揮 | 三菱総合研究所　新　誠一 | 電気通信大学　佐々木貴之 | 横浜国立大学

人々の社会生活や企業の経済活動は，さまざまな社会インフラシステムによって支えられており，特に重要な電力，情報通信，金融などの 14 分野については，政府のサイバーセキュリティ戦略本部[☆1]により重要インフラ分野に指定されている．世の中では，デジタル化，デジタルトランスフォーメーション（DX）を通じた進化はとどまるところがなく，社会インフラシステムにおいても，分野によっては程度の差はあるが，その例外ではいられない．安全性・信頼性が重視される社会インフラシステムにおいては，オープン化や汎用技術によるデジタル化には保守的ではあったが，デジタルにより進化していくことは間違いないだろう．

このような中，デジタル化が先行する海外を中心に社会インフラシステムやそのサプライチェーンに対する大規模なサイバー攻撃が増加し，インフラの機能停止に至る事故・脅威が拡大している．社会インフラシステムの機能が停止，低下した場合には，相互依存関係にある他のインフラシステムや社会経済活動に波及的に影響し，甚大な被害をもたらすリスクがある．

一方で，日本を含む世界の情勢を見渡すと，新型コロナ禍後のニューノーマルを見据えた社会・経済の大きな構造転換，カーボンニュートラルに向けた国際的な潮流による産業構造の大転換，産業インフラのデジタル化・高度化とそれらに対する大規模サ

☆1　国全体のサイバーセキュリティにかかわる司令塔．

イバー攻撃による事故・脅威の拡大，グローバルなサプライチェーンの深化と国際情勢の変化に伴う産業物資サービス等の供給体制の脆弱性の顕在化などの課題に直面している．将来世代を含む人類が直面する課題に対して、これからの新しい国際社会の在り方を方向付ける SDGs[☆2]（持続可能な開発目標）においては，「レジリエントなインフラ構築，包摂的かつ持続可能な産業化の促進およびイノベーションの推進を図る」ことが掲げられている．政府による経済安全保障法制の検討はこのような課題も背景として進められていると見られる．経済安全保障法制の検討においては，基幹インフラの安全性・信頼性の確保，サプライチェーンの強靭化などの取り組みが重要なものとして取り上げられている．社会インフラシステムのサイバーセキュリティはこのような経済安全保障を確保する上で根幹をなすものである．

このようなことから，本特集では，社会インフラシステムにおけるサイバーセキュリティ脅威，リスクとそれらに対する対策取り組み状況および今後の課題，展望についてまとめることとした．

社会インフラシステムは，前述の通りさまざまな分野があるが，本特集では最初の試みとして，その中でも重要で注目が集まる分野である電力，情報通信，金融，化学・石油・ガスやそれらの基盤となる産業制御システムについて取り上げたい．各テーマに関する概要は次ページにまとめている．

これらの分野のサイバーセキュリティは，多様なステークホルダによる取り組みが不可欠である．そのようなことから本特集では，インダストリ，ガバメント，アカデミアにおけるサイバーセキュリティの最前線で活躍する第一人者の知見を結集して関連分野の取り組み動向，課題，今後の展望についてまとめた．

本特集で紹介したサイバーセキュリティに関する産官学の包括的な取り組みと今後の課題への対応を推進することにより，レジリエントで持続可能なデジタル経済社会の基盤を構築し，デジタル経済安全保障を確保していくことが期待される．

（2022 年 2 月 7 日）

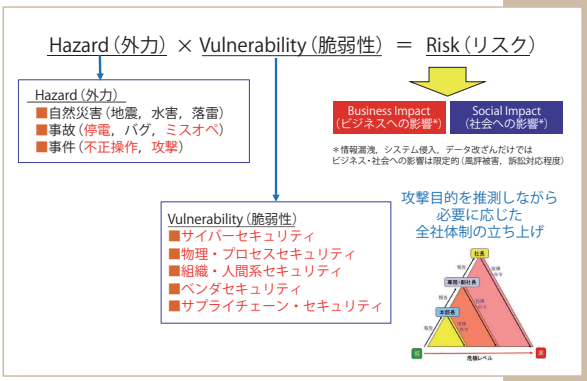
☆2 Sustainable Development Goals (United Nations)

概要

1 電力分野におけるサイバーセキュリティの現状と今後の展望
—社会インフラシステムの要（かなめ）としての役割—

渡辺研司 | 名古屋工業大学大学院社会工学専攻

電力分野は機能の停止や低下が国民生活や経済活動に大きな影響を及ぼすため，重要インフラの中でも要（かなめ）と言える．このためサイバー攻撃の標的にもなりやすく，民業だけでは太刀打ちできない状況に陥いる可能性も高いことから，官民連携のさらなる加速と演習等による実効性の担保が急がれる．またサイバー・フィジカル両面のセキュリティを確保するためには「地域」という観点での重要インフラ事業者間の連携も重要である．



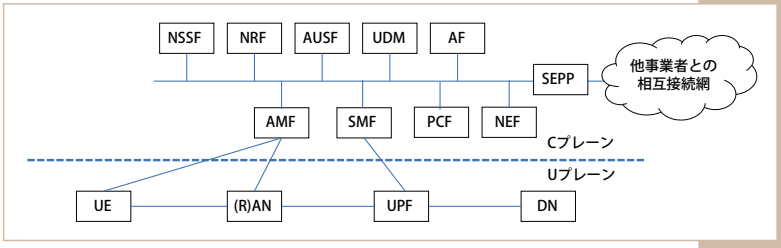
2 クラウドファースト時代のサイバーセキュリティ
—サイバーセキュリティのためのマルチステークホルダアプローチ—

石黒正揮 | 三菱総合研究所

システムを構築する際に，クラウド基盤の利用を前提に考えるべき「クラウド・ファースト」時代が到来している．クラウドを活用することでシステムを機動的に低コストで構築できるメリットは大きいが，共有リスク，協業リスクなどクラウド特有のリスクが拡大している．本稿では，クラウド特有のリスクを挙げそれらに対する技術対策およびマルチステークホルダによるセキュリティ確保に関する動向，課題，今後の展望について示す．

3 5G 移動通信システムのサイバーセキュリティ
—移動通信におけるセキュリティ対策の変遷とこれから—

窪田　歩 | （株）KDDI 総合研究所



5G は高速大容量通信，多接続，高信頼・低遅延の実現により新たなサービスの創出を促進することが期待されるとともに，今後のさまざまな分野の DX を支える基盤として重要な社会インフラとなっていくことが予想される．本稿では，移動通信システムにおけるセキュリティ対策の変遷を振り返り，5G におけるセキュリティ強化ポイント，5G システムの構築・運用における課題，5G セキュリティに関する国内外の動向について解説する．

概要

4 化学プラントのサイバーセキュリティ
― OT システムのセキュリティ脅威に対する取り組みと今後の展望―

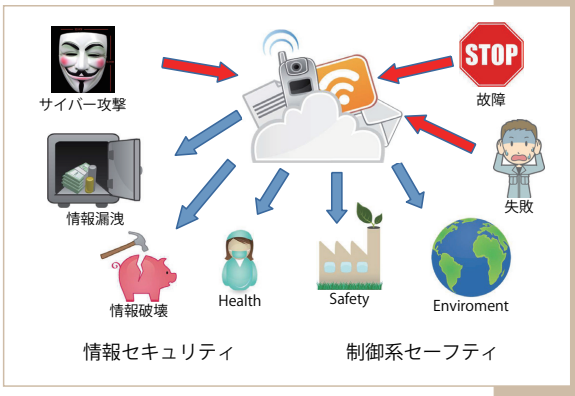
星野浩志　秋元新哉　横河電機（株）

ここ数年のサイバー攻撃者の OT 領域の知識の深化と，サイバー攻撃による社会生活への影響の発生事例を見ると，化学･石油プラントを取り巻くサイバーセキュリティ脅威は確実に進化していると言える．この事態に対応していくためには，OT 分野のシステム・機器の知見や運用現場の人・プロセス・技術の知見と，IT 分野の知見の両方が必要になる．本稿では，IT 分野の読者に向けて化学プラントの生産制御システムのサイバーセキュリティ関連の動向および課題と今後の展望について紹介する．

5 産業制御システムセキュリティの動向

新　誠一　電気通信大学

ネットワーク接続が前提となるに従い産業制御システムもサーバセキュリティ対策が不可欠になってきた．この動向と対策を概観する．合わせて，サイバーセキュリティ対策とは情報セキュリティ対策と機能安全の融合であることを再度宣言し，安全．安心な社会構築に向けての方向性を明確化する．



6 金融分野におけるサイバーセキュリティを巡る国際的な議論の動向

河田雄次　金融庁

本稿は，金融分野におけるサイバーセキュリティを巡る国際的な議論の動向について概説する．近年，サイバー攻撃の脅威が増し，金融システムの安定等にも影響を与えかねないことから，G20 や G7 等のさまざまな場において，サイバーセキュリティ対策，規制報告枠組み，第三者委託，犯罪収益など多面的な観点から議論が行われている．引き続き，金融当局が連携して，課題解決に向けた議論をグローバルに深めていくことが望まれる．