RFC2350 コンピュータセキュリティインシデント対応への期待

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	対応チーム の種類にかかわらず、それにサポートされているコミュニティは、そのチームのポリシーと手続きを知っておかなければなりません。		○				○
	その情報が取得された入手元がどこであれ、そのテンプレートのユーザは、その真正性をチェックしなければなりません。		○				○
	そのような相互関係を支援するための協力関係を築く際に、CSIRT は安全に護るべき情報を共有するために、どのような種類の契約が両者間に存在しうるか、この関係が開示されうるか、この場合誰に対してか、を 決めなければなりません。		○				○
	変造した電子メールを送ることは、非常に簡単で、電話で（虚偽の）身元をつくろうことは難しいことではありません。暗号技術、例えば PGP （ Pretty Good Privacy ）もしくは PEM（ Privacy Enhanced Mail ）は、 電子メールをセキュアにする有効なやり方を提供することができます。 正しい機器をもつことによって、電話のコミュニケーションもセキュアにすることができます。しかし、そのような機構を使う前に、双方の主体が「正しい」基盤を必要とします。つまり、事前の準備です。最も重要な準備は、セキュアなコミュニケーションで使用される暗号鍵の真正性を確認することです。: － 公開鍵（ PGP や PEM のような技術のためのもの）: これらはインターネット上のどこからでもアクセスできるので、公開鍵は 使用する前に認証されなければなりません。（ユーザが他の人の鍵に署名 する）PGP は「信頼の蜘蛛の巣」に依存する一方、（ CA 局がユーザの鍵に署名する）PEM は、階層構造に依存します。 － 秘密鍵（ DES や PGP/ コンベンショナル暗号化のような技術のためのもの）: これらは送り手と受け手の双方が知っていなければならないので、秘密鍵はコミュニケーションの前にセキュアなチャネルを通じて交換されなければなりません。	○				○	
	セキュアなコミュニケーションの技術的問題や管理的問題に対応することは、本書の範囲外です。要点は、対応チームは、自身や彼らの構成員 （あるいは他の対応チーム)との間のコミュニケーションをセキュアに する手段をサポートし、使用しなければならないということです。機構が何であれ、それが提供する保護のレベルは、構成員のコミュニティが許容できるものでなければなりません。		○				○
	CSIRT の詳細は、時間の経過に伴って変化するので、埋められたテンプレートには、いつ最後に更新されたかが含まれなければなりません。		○				○
	CSIRT への連絡方法の完全な詳細は、チームごとにまちまちでしょうが、ここに掲載される必要があります。		○				○
	何らかのサービスへのアクセスに特定の手続きがある場合（例: メーリングリストの要求に対応する場合）、それらはここで説明される必要があります。		○				○
	使命の表明は、CSIRT の規定によって既に開始されているチームの核となる活動に焦点を当てる必要があります。CSIRT としてみなされるためには、そのチームは、インシデントの報告をサポートし、インシデントを扱うことによってその構成員をサポートしなければなりません。		○				○

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	構成員の定義は、誰にそのチームはサービスを提供するのかに関してグループの周囲に境界を作る必要があります。この文書のポリシーの章（後述）では、この境界の外部からの要求がどのように扱われるかが 説明される必要があります。		○				○
	CSIRT がその構成員を開示しないことを決定した場合、この決定の背後にある理由付けを説明する必要があります。		○				○
	ISP が CSIRT を提供する場合、CSIRT を持った顧客サイトにもサービスを提供するので構成員は重複している可能性があります。CSIRT の記載（後述）のオーソリティの章は、そのような関係を明確にする必要が あります。						○
	CSIRT の活動をオーソライズするスポンサー組織が次に掲げられる必要があります。これを知っておくことは、CSIRT の背景と設立を理解することを助け、構成員と CSIRT 間の信頼を築くための決定的な情報です。		○				○
	CSIRT は、その境界内のすべてのシステムの運用において介在するオーソリティを持っている場合もあれば、無い場合もあります。それは、その構成員の境界で区別される、そのコントロールの範囲を識別する必要があります。他の CSIRT が、その境界内で階層的に運用する場合には、これはここに記述され、関連する CSIRT が識別される必要があります。		○				○
	チームのオーソリティの開示は、自身を義務としての要求にさらすことになるでしょう。各チームは、このような事柄については法的な助言を仰ぐ必要があります。		○				○
	そのチームが対応することができるインシデントの種類と、各種のインシデントに対応するときにそのチームが提供するサポートのレベルは、一覧形式でここに示される必要があります。サービスの章（後述）では、より詳細な記述を与える機会を提供し、インシデントに関連しない話題に対応します。		○				○
	サポートのレベルは、チームの仕事量や、入手可能な情報の完全性のような要素によって変化することでしょう。このような要素は、概略が 述べられる必要があり、それらの影響が説明される必要があります。		○				○
	既知の種類のインシデントについてのリストが、潜在的な、もしくは 将来のインシデントに関して不完全であるのと同様に、CSIRT は、さもなければ言及されることのない種類のインシデントに対する「デフォルト」サポートについて、何らかの背景を提供する必要もあります。		○				○
	そのチームは、彼らが受け取る将来のインシデントの可能性を作り出す脆弱性の情報について、行動を起こすか否かについて表明する必要があります。		○				○
	この章では、どの関係グループとその CSIRT は、規則的に相互関係をもっているかを明確にする必要があります。		○				○
	報告と開示のポリシーは、各状況下において、誰が CSIRT の報告の受取人となるかを明確にする必要があります。		○				○
	そのチームが他の CSIRT 経由で運用することを予定しているのか、あるいは他の構成員のメンバーと直接、そのメンバーに個別的に関係のある事項について運用することを予定しているのかを明記しておく必要もあります。		○				○
	CSIRT は、しばしば他の CSIRT と相互関係をもつ必要があります。		○				○
	例えば、大企業内の CSIRT は、インシデントを国レベルの CSIRT に報告する必要があるかもしれません		○				○

RFC2350 コンピュータセキュリティインシデント対応への期待

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	国レベルの CSIRT は、大規模な攻撃に巻き込まれたすべてのサイトを扱うために、外国の国レベルの CSIRT にインシデントを報告する必要があるかもしれません						
	ベンダーには自前の CSIRT をもっているところがありますが、もっていないベンダーもあります。そのような場合、CSIRT は、その技術的な 問題を分析したり、もしくは提供された解消法をテストするように、 改善もしくは修正を提案したり、ベンダーとともに直接、働く必要があるでしょう。		○				○
	CSIRT やテンプレートのユーザは、国ごとに相当に異なるであろう現地の法規や規制に敏感である 必要があります。		○				○
	CSIRT には、報道関係者がひっきりなしに情報やコメントを求めてアプローチしてきます。報道機関に対する開示に関する明確なポリシーは、有用である可能性があります。特に CSIRT の構成員の期待を明確にする際にはいえます。報道ポリシーは、上記と同様の話題について、より具体的に明確化する必要があるでしょう。		○				○
	CSIRT のテンプレートは、どの情報を、誰に、いつ報告ないし開示するかを定義する必要があります。		○				○
	各チームのテンプレートは、ユーザの期待を明確化する目的と、他のチームに知らせる目的の両方のために、いかなる、そのような制約を規定する必要があります。		○				○
	チームは、通常、統計情報を集めます。統計情報が配布されている場合、そのテンプレートの報告と開示のポリシーには、そのように書かれる必要があり、そのような統計情報を入手する方法を記述する必要があります。		○				○
	あなたが使用するセキュアで検証可能なコミュニケーション手段を記述するポリシーを持たねばなりません。これは、CSIRT 間と、CSIRT とその構成員 間のコミュニケーションに必須です。テンプレートには、公開鍵、もしくはそれらへのポインターが、鍵のフィンガープリントを含めて含まれている必要があります。これには、真正性をチェックするためにこの情報の使う方法と、壊れた情報の扱い方（例えば、どこにこれを報告するか）についてのガイドラインが伴っている必要があります。		○				○
	現時点では、最低限、各 CSIRT が（可能であれば）PGP 鍵を入手可能にすることが推奨されます。チームによっては、自身のニーズや、その構成員のニーズに従って、他の機構（例： PEM、MOSS、S/MIME ）も利用可能にするかもしれません。しかし、CSIRT やユーザは、現地の法や規制に敏感である必要があることを覚えておいてください。国によっては強い暗号を許していなかったり、または暗号技術の利用にあったって特定のポリシーが強制されています。取り扱いに注意を要する情報を、暗号化可能な限り暗号化することに加えて、書簡がデジタル署名を含んでいる必要があります。	○	○			○	○
	そのチームのオンラインの情報サービスを通じて様式を提供するのが最も効率的です。それらへの正確なポインターは、適切な使用法についての表明と、何時、どのようにその様式を使うかのガイドラインとともに CSIRT 概要の文書中に掲載される必要があります。独立した電子メールアドレスが、様式に基づいた報告においてサポートされている場合、それらもここに掲載される必要があります。		○				○
	CSIRT の記述文書は、契約を構成するものではありませんが、義務は、おそらくそのサービスや目的の記述によることでしょう。それゆえ、免責についてをテンプレートの末尾に含めることが推奨され、制限の可能性についてユーザに警告する必要があります。		○				○

参照資料	管理策	医療機関		ルータ製造・販売事業者		ISP/NW事業者	
		機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール	機器に関する技術仕様	運用ルール
	免責についての記述による保護の使用は、各 CSIRT が認識している必要がある現地の法や規制によって影響を受けます。迷う場合には、その CSIRT は法律家に免責について確認する必要があります。		○				○