Hướng dẫn Thành lập CSIRT

Bản 2.0
VietnameseVersion 1.0

Translated by VNCERT and NTT East Corporation

MỤC LỤC

Các Phiên bản của Tài liệu

Bản	Ngày	Mô tả
1.0 vn	27/07/2016	Bản dịch tiếng Việt của VNCERT
2.0	01/08/2011	Bản tạo bởi NCA.
1.0	05/02/2007	Tạo mới.

Acknowledgements
Translated into English supported by NTT EAST Corporation and VNCERT
Translated into Vietnamese supported by NTT EAST Corporation and VNCERT

1 Lời nói đầu

Tài liệu này mô tả những vấn đề cần được giải quyết cẩn thận và cần được định nghĩa khi thành lập một đội ứng cứu sự cố bảo mật máy tính (CSIRT) tại Nhật Bản. Tài liệu cũng đề cập đến những quy trình nên được tuân theo khi xây dựng kế hoạch ứng cứu sự cố trong một tổ chức nhằm mục đích sử dụng như là một hướng dẫn chung để thành lập CSIRT.

Không thể có hai mô hình CSIRT giống hệt nhau do tính duy nhất về mục tiêu và bối cảnh của tổ chức. Do đó, cũng không thể có hai nhóm hoạt động theo cách thức giống nhau hoàn toàn. Để CSIRT hoạt động hiệu quả nhất, cần làm rõ các yếu tố sau: là một tổ chức riêng, lý do tại sao phải phát triển thành CSIRT và CSIRT cần đạt được điều gì. . Tài liệu này nhằm để những người tham gia thành lập CSIRT tại Nhật Bản sử dụng như một nguồn lực khi xem xét những tiêu chí phù hợp cho từng loại tổ chức.

Tài liệu này dùng cho các quản trị viênvà nhân viên tại Nhật Bản, những người có trách nhiệm thực hiện các biện pháp của tổ chức để ngăn ngừa các sự cố bảo mật lặp lại và nhằm hạn chế thiệt hại phát sinh do sự cố. Chúng tôi mong rằng tài liệu này có thể được sử dụng một cách hiệu quả để tăng cường bảo mật.

Trong khuôn khổ chương trình hợp tác APT (Asia Pacific Telecommunity) giữa Nhật Bản gồm Hiệp hội CSIRT Nhật Bản NCA (Nippon CSIRT Association), Trung tâm Điều phối các Đội Ứng cứu Khẩn cấp Máy tính Nhật Bản JPCERT/CC (Japan Computer Emergency Response Team Coordination Center), Công ty NTT-East - Tập đoàn viễn thông NTT Nhật Bản và Việt Nam với đại diện là Trung tâm Ứng cứu Khẩn cấp Máy tính Việt Nam VNCERT (Vietnam Computer Emergency Response Team) thuộc Bộ Thông tin và Truyền thông Việt Nam, tài liệu này được chuyển sang phiên bản tiếng Việt để hỗ trợ cho việc phát triển CSIRT tại các doanh ngiệp và tổ chức tại Việt Nam.

2 CSIRT và Hoạt động Ứng cứu Sự cố Bảo mật

Với sự tiến bộ đáng kể gần đây về công nghệ thông tin, các hệ thống thông tin đang đóng vai trò ngày càng quan trọng và thông tin từ các hệ thống này rất cần thiết cho các hoạt động của doanh nghiệp. Vì thế, những tổ chức không có công cụ để xác định được nguyên nhân của sự cố bảo mật máy tính (gọi tắt là "Sự cố") hoặc không có kế hoạch cải tiến hệ thống phù hợp có thể dẫn đến giảm năng suất, đánh mất sự tin tưởng và tín nhiệm của xã hội, trong một số trường hợp phải trả chi phí cao cho các đơn vị bên ngoài do những thiệt hại, hay phải đối diện với những tình huống đe dọa đến sự tồn tại của tổ chức do Sự cố, gây tác động đáng kể đến việc kinh doanh.

Không một tổ chức nào có khả năng thực hiện tất cả những biện pháp bảo mật để ngăn ngừa mọi Sự cố tiềm tàng. Hơn nữa, do các hệ thống ngày càng phức tạp nên không thể loại trừ khả năng xảy ra Sự cố cho dù hệ thống thông tin có được xây dựng và vận hành bảo mật đến thế nào.

Một Đội Ứng cứu Sự cố Bảo mật Máy tính (gọi tắt là "CSIRT") là một tổ chức không chỉ tiến hành việc phân tích và ứng cứu đối với các Sự cố thực tế, mà còn tiến hành các hoạt động như đào tạo và giám sát để tăng cường chất lượng bảo mật. Các hoạt động này nhằm mục đích thực hiện Ứng cứu[1] Sự cố hiệu quả và giảm thiểu những rủi ro như đã nêu trên.

Thành lập CSIRT sẽ mang đến những lợi ích sau đây:

- ✓ Phát hiện Sự cố, Sự kiện Bảo mật[22] và chuyển thông tin nhanh chóng, chính xác đến tổ chức;
- ✓ Tích lũy và chia sẻ kinh nghiệm ứng cứu Sự cố;
- ✓ Tăng cường chất lượng bảo mật để ngăn Sự cố tái diễn.

Hầu hết các công ty đều đã có biện pháp ứng phó với các Sự cố. Tuy nhiên, thường chỉ ở cấp bộ phận và chỉ một vài công ty mới có mô hình ứng phó Sự cố trong toàn tổ chức. Vì vậy, nhu cầu cấp thiết là thành lập đội CSIRT để ứng cứu Sự cố trong toàn công ty với các nguồn lực hiện có.

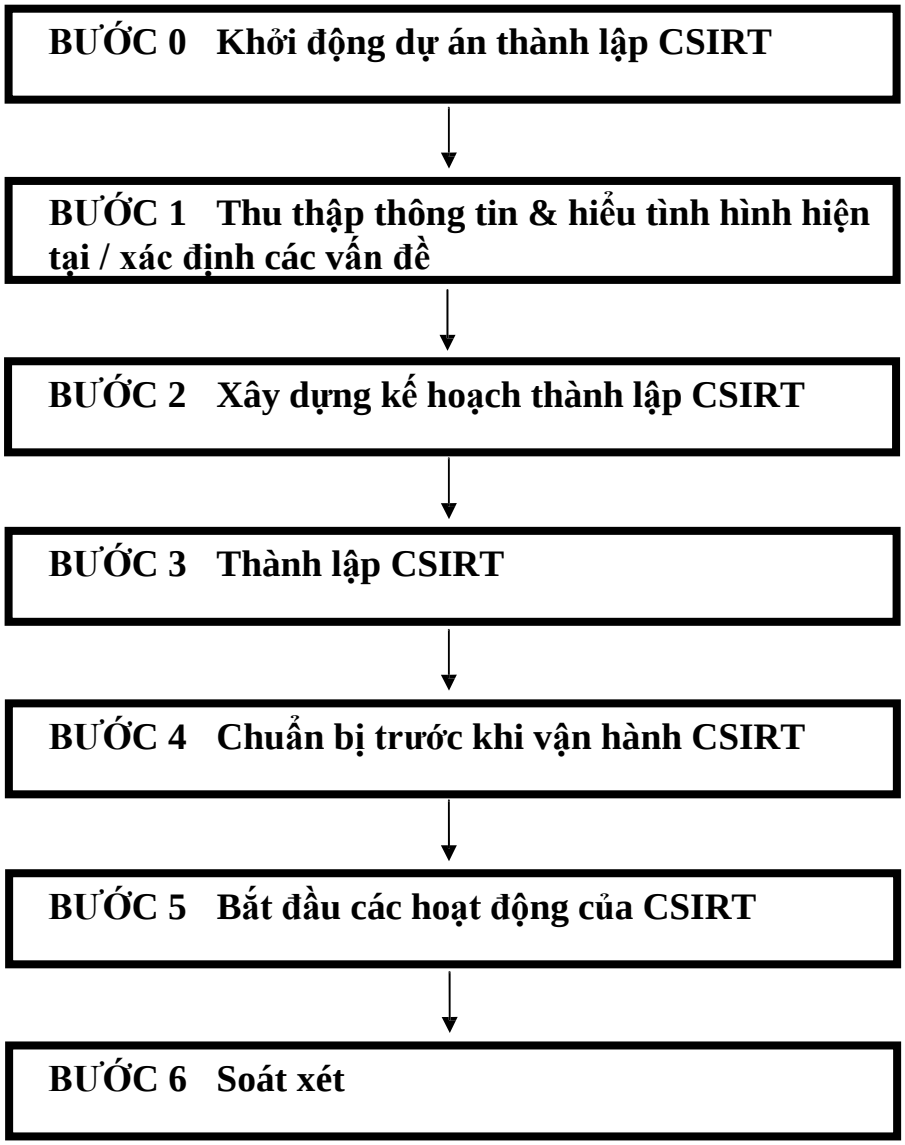
Đôi khi, chỉ một Sự cố cũng có thể đe dọa đến sự tồn tại của công ty nên các biện pháp ứng phó không được phép sai sót. Khi một công ty thành lập CSIRT và thiết lập cơ chế ứng phó Sự cố phù hợp, năng suất sẽ được cải thiện, công ty sẽ có thêm sự tin tưởng từ xã hội và đạt được những mục tiêu kinh doanh của mình.

[1] Hoạt động ngăn ngừa và khắc phục Sự cố

[2] Với mục đích của tài liệu này, "Sự kiện Bảo mật" được định nghĩa là một sự kiện có khả năng, nhưng chưa được xác định chính xác là một Sự cố

3 Các bước Thành lập CSIRT

Cách thức thành lập CSIRT tùy thuộc vào môi trường vốn có của tổ chức như trình độ chuyên môn của nhân viên hay tiềm lực tài chính. Tiến trình sau đây thể hiện những bước liên quan đến việc thành lập một CSIRT, là những bước cơ bản áp dụng cho bất kỳ tổ chức nào:



4 Tiến trình chi tiết Thành lập CSIRT

Phần này mô tả chi tiết các bước đã thể hiện trong phần **3 - Các bước Thành lập CSIRT.**

BƯỚC 0 Khởi động dự án thành lập CSIRT

Ở BƯỚC 0, khởi động "dự án thành lập CSIRT" là thực hiện các hoạt động liên quan đến việc thành lập CSIRT. Những điểm sau cần được xem xét để thuận tiện cho tiến độ dự án:

(1) Mục đích (Để thành lập CSIRT)
- Làm rõ lý do thành lập CSIRT

(2) Thành viên dự án:
- Bao gồm những thành viên liên quan đến các Sự cố bảo mật;
- Làm rõ tầm quan trọng của các thành viên;
- Đảm bảo phương tiện thông tin liên lạc cho thành viên ở xa;
- Thiết lập cơ chế để tuy xuất nhanh các ý kiến chuyên môn hay các quan điểm khi cần.

(3) Lập kế hoạch
- Xác nhận các ràng buộc về thời gian.

(4) Vận hành dự án
- Làm rõ những nguyên tắc vận hành;
- Xác nhận các tiến trình ra quyết định trong dự án;
- Những hạn chế.

Cần có được sự phê duyệt từ ban giám đốc hoặc người ra quyết định khi khởi động dự án thành lập CSIRT.

BƯỚC 1 Thu thập thông tin & hiểu tình hình hiện tại / xác định các vấn đề

BƯỚC 1 bắt đầu bằng việc khảo sát bối cảnh của CSIRT sẽ được thành lập và tình hình hiện tại của doanh nghiệp. Dựa trên kết quả khảo sát, xác định những hoạt động cần đạt được và những vấn đề có thể phát sinh khi thành lập CSIRT.

Dưới đây là ví dụ về những thông tin cần thu thập để thể hiện tình hình hiện tại của tổ chức. Có thể tham khảo “Phụ lục (1) Chi tiết về thông tin cần thu thập, tình hình hiện tại, và xác định các vấn đề - Hướng dẫn Khởi động CSIRT”

- ✓ Xác định những tài sản thông tin cần được bảo vệ và những mối đe dọa
- ✓ Thông tin về cơ chế phản ứng Sự cố hiện có
- ✓ Thông tin về những chính sách hiện có và những tài liệu liên quan đến bảo mật
- ✓ Thông tin tham khảo

Sau đó, chọn ra những vấn đề hiện tại dựa trên thông tin đã thu thập được và tiến hành một đợt xem xét để thành lập CSIRT. Sau đây là những ví dụ về những vấn đề cần được xem xét khi thành lập CSIRT.

- ✓ Nhu cầu cơ bản của việc thành lập CSIRT là gì?
- ✓ Những loại dịch vụ nào nên được đưa ra?
- ✓ CSIRT nên được đặt ở đâu trong tổ chức?
- ✓ CSIRT cần có quy mô như thế nào?
- ✓ Thành lập CSIRT tốn bao nhiêu chi phí?

Dựa trên kết quả xem xét về những vấn đề trên, xây dựng kế hoạch thành lập CSIRT như BƯỚC 2 dưới đây.

BƯỚC 2 Xây dựng kế hoạch thành lập CSIRT

(1) Xem xét những ý tưởng cơ bản của CSIRT
(2) Xem xét dịch vụ sẽ được cung cấp
(3) Xem xét cấu trúc nội bộ công ty
(4) Xem xét sự phối hợp bên ngoài
(5) Xem xét các nguồn lực
(6) Xem xét sự khác biệt giữa CSIRT lý tưởng và CSIRT sẽ được thành lập
(7) Xem xét tiến độ thành lập CSIRT

Trong BƯỚC 2, xây dựng kế hoạch thành lập CSIRT mô tả CSIRT cần được thành lập theo kiểu nào để giải quyết những vấn đề và khó khăn đã xác định trong BƯỚC 1. Quy trình phát triển kế hoạch để thành lập CSIRT được thể hiện dưới đây:

(1) Kiểm tra những ý tưởng cơ bản của CSIRT

Thông qua việc phác thảo những ý tưởng cơ bản của CSIRT, làm rõ định hướng của CSIRT sẽ được thành lập và kiểm tra những ý tưởng đó của CSIRT để có được hiểu biết cơ bản về những mục tiêu sẽ đạt được.

● **Xác định Đối tượng phục vụ (bên nhận dịch vụ)**

Đối tượng phục vụ là các nhóm hay tổ chức có thể sử dụng các dịch vụ nhất định do CSIRT đưa ra. Việc xác định đối tượng phục vụ là một yếu tố chính trong việc xác định rõ định hướng của CSIRT sẽ được thành lập.

Ví dụ tham khảo về đối tượng phục vụ:

Đối tượng phục vụ của ABC-CSIRT
Các quản trị viên hệ thống thông tin, người chịu trách nhiệm vận hành, người dùng và quản trị viên bảo mật làm việc cho ABC

● **Xác định nhiệm vụ**

Các nhiệm vụ chi tiết cần xác định khi thành lập CSIRT:

- Tình hình hay vị trí hiện tại của tổ chức
- Những phương tiện được sử dụng để đạt được các mục tiêu
- Những mục tiêu sẽ đạt được

Tuỳ theo bối cảnh của tổ chức sẽ thành lập CSIRT nên mục tiêu chính cần đạt của CSIRT sẽ khác nhau nhưng có thể tóm tắt chủ yếu như sau:

- Tiến hành các hoạt động để ngăn sự xuất hiện / lặp lại sự cố
- Giới hạn thiệt hại do các Sự cố gây ra và giảm thiểu mất mát bằng cách thực

hiện ứng cứu phù hợp và biện pháp hiệu quả.

Nhiệm vụ được xác định cho từng tổ chức nên rõ ràng và súc tích về những quy trình cụ thể để đạt được thành quả cũng như những mục tiêu cụ thể cần đạt được. Nhiệm vụ cũng cần chỉ ra cách CSIRT sẽ tương tác như thế nào với đối tượng phục vụ.

Một ví dụ về nhiệm vụ được đưa ra dưới đây để tham khảo:

Nhiệm vụ của ABC-CSIRT
Nhiệm vụ của chúng tôi là góp phần tăng cường bảo mật tại ABC và mạng xã hội bằng cách nhận vai trò chính trong lĩnh vực bảo mật tại ABC, là đầu mối phối hợp với những tổ chức và chuyên gia tại ABC cung cấp dịch vụ tư vấn về bảo mật thông tin; hỗ trợ việc phát hiện, giải quyết, hạn chế thiệt hại, và ngăn chặn những Sự cố bảo mật.

- **Xác định những sự cố cần xử lý**

  Là quyết định vấn đề nào trong BƯỚC 1 cần được CSIRT giải quyết, và xác định những Sự cố cần xử lý, giúp kiểm tra các dịch vụ và các nguồn lực, ... mà CSIRT cần có trong chức năng của nó.

  “Phụ lục (2) Phân loại Sự cố - Hướng dẫn Thành lập CSIRT” cung cấp tham khảo về phân loại Sự cố cần xử lý. Tuy nhiên, cần nhận thức rằng những phân loại này được đưa ra từ quan điểm hệ thống và thiệt hại thực tế sẽ rất khác nhau tuỳ theo bản chất của hệ thống thông tin.

(2) <u>Kiểm tra những dịch vụ được cung cấp</u>

"Dịch vụ" có nghĩa là những chi tiết cụ thể về việc ứng cứu Sự cố sẽ được cung cấp bởi CSIRT. Phần sau đây phác thảo về những dịch vụ CSIRT chung. Tuy nhiên, CSIRT không nhất thiết phải cung cấp tất cả những dịch vụ này mà xem xét CSIRT cần cung cấp dịch vụ nào tùy thuộc vào đối tượng phục vụ, nhiệm vụ của nhóm và những sự cố nhóm sẽ xử lý.

Các dịch vụ CSIRT có thể được chia thành ba loại chính:

- **Dịch vụ khắc phục Sự cố**

  Loại này gồm các dịch vụ ứng cứu những Sự cố và sự kiện liên quan đến Sự cố nhằm giới hạn thiệt hại gây ra bởi các Sự cố.

- **Dịch vụ ngăn ngừa Sự cố**

  Loại này gồm các dịch vụ phát hiện và giảm thiểu nguy cơ xảy ra các Sự cố và sự kiện bảo mật nhằm ngăn chặn các Sự cố xảy ra.

- **Dịch vụ tăng cường chất lượng bảo mật**

  Loại này gồm các dịch vụ nhằm nâng cao chất lượng bảo mật nội bộ. Chúng cung cấp những hiểu biết từ cơ bản đến chuyên sâu của CSIRT để các hoạt động có thể được thực hiện thông qua sự phối hợp trong các tổ chức nội bộ. Chúng cũng có thể gián tiếp ngăn ngừa xảy ra Sự cố.

Bảng 1 trình bày danh sách những dịch vụ điển hình. Một CSIRT không nhất thiết phải có tất cả các dịch vụ này và trong một số trường hợp có thể đưa thêm những dịch vụ khác. (Chi tiết các dịch vụ, xem "Phụ lục (3) Dịch vụ - Hướng dẫn thành lập CSIRT.")

Dịch vụ khắc phục Sự cố	Dịch vụ ngăn ngừa Sự cố	Dịch vụ tăng cường chất lượng bảo mật
• Xử lý Sự cố	• Cung cấp thông tin liên quan đến bảo mật	• Phân tích / đánh giá rủi ro
• Điều phối	• Xử lý thông tin lỗ hổng	• Chuẩn bị và sửa đổi những kế hoạch duy trì kinh doanh và khôi phục thảm hoạ
• Điều tra số máy tính	• Phát hiện Sự cố / Sự kiện Bảo mật	•Tư vấn bảo mật
• Ứng cứu Sự cố tại chỗ	• Khảo sát xu hướng kỹ thuật	• Các hoạt động huấn luyện / đào tạo / hướng dẫn về bảo mật
• Hỗ trợ ứng cứu Sự cố	• Đánh giá / kiểm tra bảo mật	• Chứng nhận / đánh giá sản phẩm
• Xử lý nhân công	• Phát triển công cụ bảo mật	

Bảng 1: Phác thảo về các dịch vụ của CSIRT

Đồng thời với việc xem xét các dịch vụ sẽ được cung cấp cũng phải xem xét thẩm quyền cho phép CSIRT cung cấp dịch vụ. Việc xử lý Sự cố[3] là rất quan trọng và phải được thực hiện bởi CSIRT. Do vậy, CSIRT phải thiết lập các quy trình xử lý sự cố.

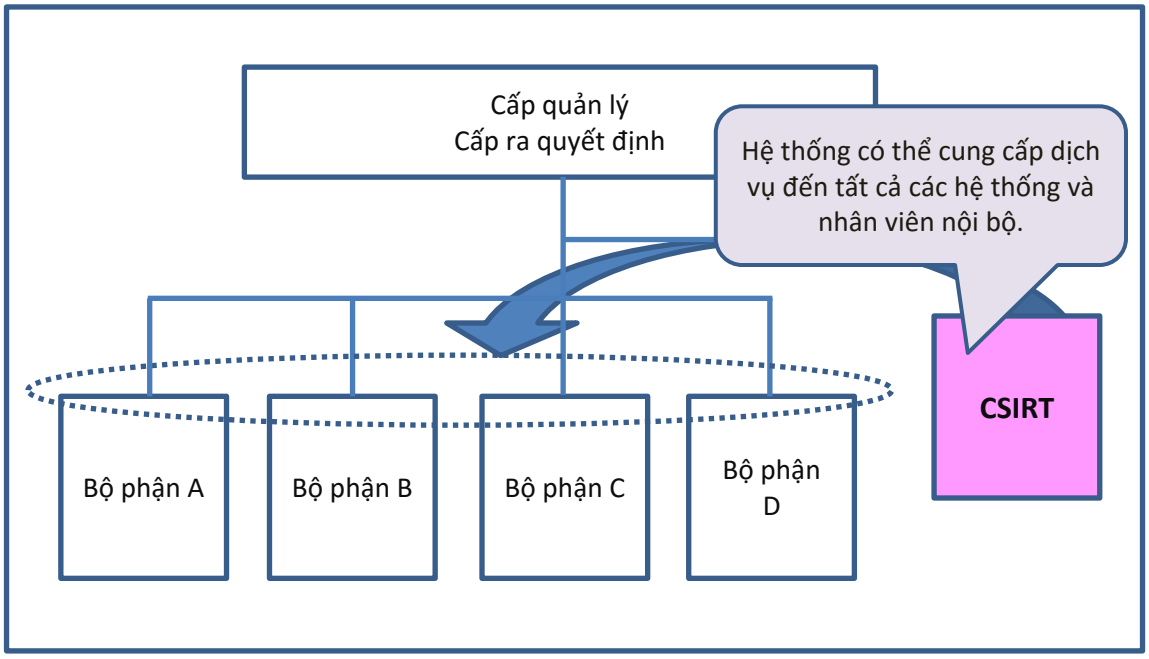
Nếu đã có sẵn các chức năng xử lý Sự cố trong nội bộ, tổ chức cần sử dụng hiệu quả những chức năng này và kiểm tra mối tương quan của chúng với CSIRT. Cần xem xét cách chuyển những chức năng phản ứng Sự cố hiện có cho CSIRT theo yêu cầu.

(3) Kiểm tra cơ cấu tổ chức của công ty

Kiểm tra cơ cấu tổ chức của công ty để xác định CSIRT sẽ có chức năng như thế nào. "Phụ lục (4) Các bộ phận liên quan đến phản ứng Sự cố - Hướng dẫn Thành lập CSIRT" đưa ra danh sách những bộ phận cần đưa vào cơ cấu tổ chức của công ty.

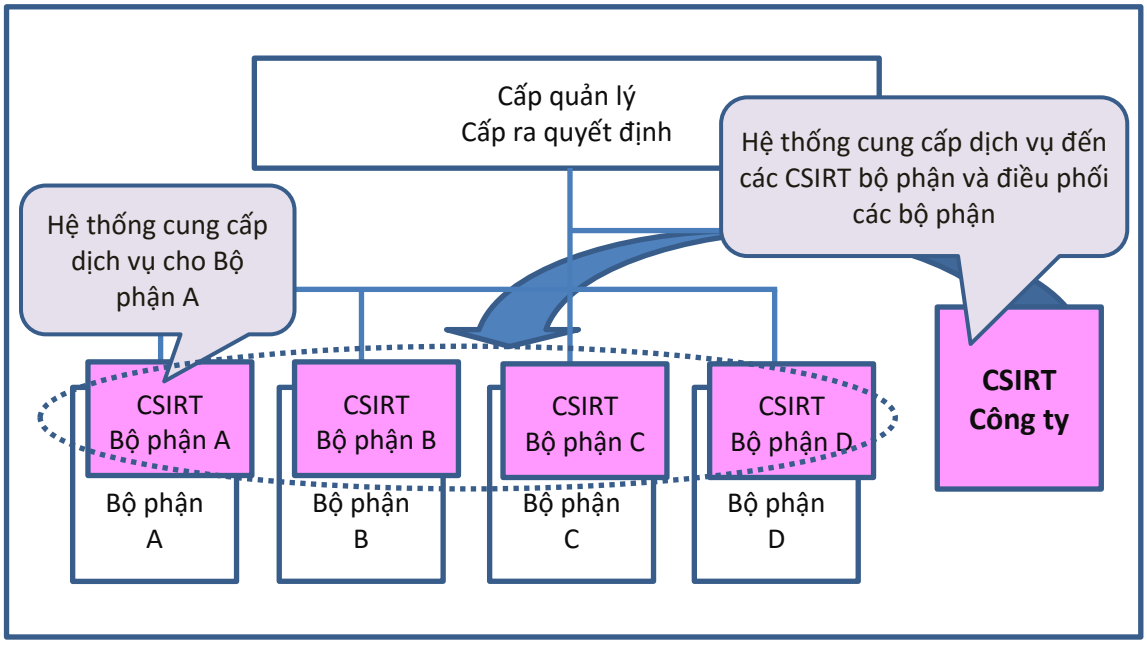
Ví dụ, nếu tất cả những hệ thống và nhân viên nội bộ đều là đối tượng phục vụ từ CSIRT, phải có một mô hình hoạt động cho phép cung cấp dịch vụ đến các đối tượng này. Mô hình như trong Hình 1 dưới đây.

[3] Ứng cứu Sự cố phát sinh và những hoạt động để giới hạn thiệt hại và phục hồi.



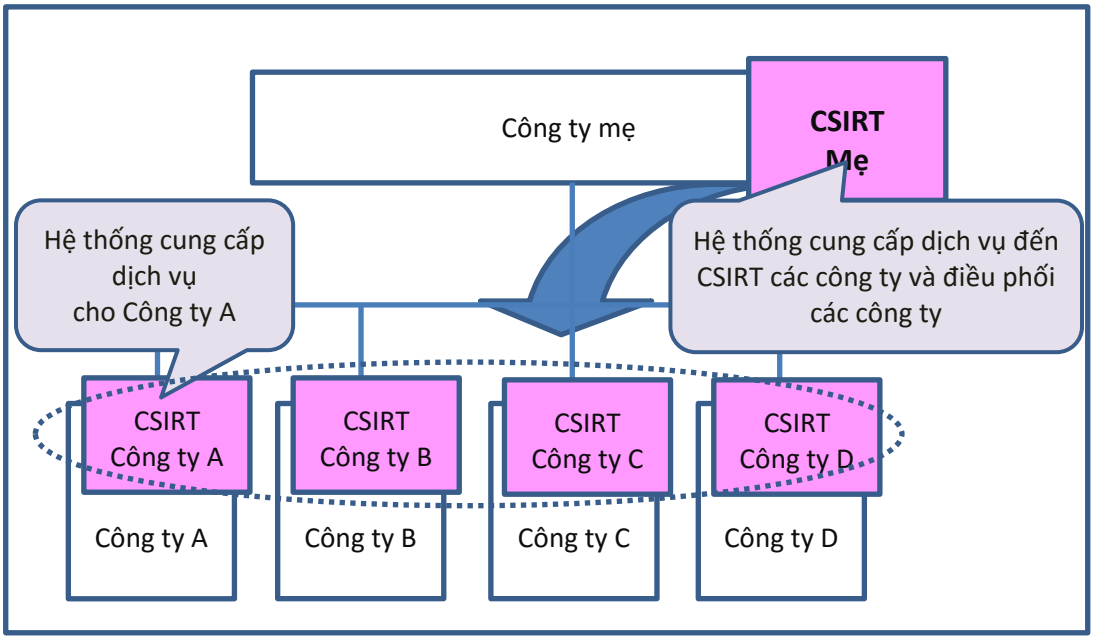
Hình 1: Mô hình cho Doanh nghiệp - các hệ thống và nhân viên nội bộ đều là đối tượng phục vụ

Hơn nữa, nếu CSIRT gặp khó khăn trong việc cung cấp dịch vụ cho tất cả các hệ thống và nhân viên nội bộ do tổ chức có quy mô lớn, thì mô hình như trong Hình 2 có thể sẽ hiệu quả hơn. Với mô hình này, thành lập CSIRT cho mỗi bộ phận và một CSIRT để điều phối ở quy mô toàn công ty.



Hình 2: Mô hình cho Doanh nghiệp lớn - mọi hệ thống và nhân viên nội bộ đều là đối tượng phục vụ

Một mô hình CSIRT phân cấp tương tự như Hình 2 có thể hoạt động hiệu quả đối với CSIRT của một tổ chức có nhiều công ty cùng tập đoàn, trong đó tất cả các công ty đều là đối tượng phục vụ của CSIRT. Hình 3 thể hiện mô hình trường hợp này:



Hình 3: Mô hình cho tập đoàn - tất cả các công ty trong tập đoàn đều là đối tượng phục vụ

Khi xem xét mô hình nội bộ, cần thể hiện các điểm sau: quyền của CSIRT, các hệ thống được liên kết, các điểm kết nối giữa CSIRT và các bộ phận với chức năng ứng cứu sự cố hiện tại.

Ngoài ra, cũng cần kiểm tra nơi CSIRT nên được đặt.

(4) Kiểm tra sự phối hợp bên ngoài

Trong một số trường hợp, các hoạt động ứng cứu Sự cố có thể có sự phối hợp với các đơn vị bên ngoài. Do đó, cần xem xét mô hình phối hợp với các tổ chức bên ngoài.

- **Phối hợp với CSIRT bên ngoài**

  Phối hợp với CSIRT bên ngoài có thể giúp CSIRT hoạt động hiệu quả trong việc phát hiện Sự cố, chia sẻ bí quyết (know-how) về phản ứng Sự cố, thực hiện phối hợp xử lý Sự cố giữa các tổ chức, ... Để phối hợp hiệu quả giữa các CSIRT, cần xem xét CSIRT thuộc loại nào và cần được điều gì.

  Mô hình điển hình cho việc phối hợp giữa các CSIRT có thể ví dụ như FIRST[4] và APCERT[5]. Nippon CSIRT Association[6] đóng vai trò là một cộng đồng cho việc

[4] FIRST viết tắt cho Forum of Incident Response and Security Teams, và là một tổ chức gồm các CSIRT trên khắp thế giới. (http://www.first.org/)

[5] APCERT viết tắt cho Asia Pacific Computer Emergency Response Team, và là một tổ chức gồm các CSIRT trong khu vực Châu Á Thái Bình Dương. (http://www.apcert.org/)

[6] Nippon CSIRT Association (tên chính thức: Nippon Computer Security Incident Response Team Association; viết tắt là "NCA") là một thuật ngữ chung về tổ chức giải quyết những Sự cố liên quan đến bảo mật máy tính. Tổ chức này thực hiện

phối hợp giữa các CSIRT tại Nhật Bản.

- **Phối hợp với các tổ chức khác**

  CSIRT có thể cần đáp ứng và/hoặc phối hợp với các cơ quan thực thi pháp luật (ví dụ như cảnh sát), báo chí, và các nhà cung cấp sản phẩm trong việc ứng cứu Sự cố và cần thiết lập sẵn một chính sách về cách thức làm việc với các tổ chức bên ngoài đó.

(5) Xem xét các nguồn lực

Nên xem xét các nguồn lực cần thiết cho việc cung cấp các dịch vụ và thiết lập các mô hình nội bộ và bên ngoài, và những hạn chế về nguồn lực trong tổ chức. "Phụ lục cho Hướng dẫn Thành lập CSIRT, (5) Nguồn lực" thể hiện phác thảo về những dạng nhân lực bạn có thể cần.

- **Kiểm tra nguồn nhân lực**

  Xem xét trong mô hình tổ chức có bao nhiêu nhân viên với kỹ năng cần thiết để tiến hành các hoạt động của CSIRT. Nếu không thể đảm bảo đủ nguồn lực sẵn sàng cho công việc ứng cứu Sự cố, thì cũng cần xem xét việc đào tạo để phát triển nhân viên. Trong trường hợp này, ngoài việc phát triển nguồn nhân lực nội bộ, bạn có thể dùng hình thức đào tạo cho ứng cứu Sự cố để phát triển hiệu quả nguồn nhân lực.

- **Kiểm tra tài nguyên trang thiết bị**

  Xem xét những trang thiết bị cần có để vận hành CSIRT. Do hầu hết thông tin về Sự cố được CSIRT xử lý đều bảo mật, nên cần bố trí các trang thiết bị để ngăn chặn bất kỳ sự tiết lộ thông tin không cần thiết, thậm chí trong nội bộ công ty.

- **Ngân sách**

  Tính toán ngân sách cần cho các hoạt động CSIRT trên cơ sở chi phí cho nhân lực và trang thiết bị, cũng như chi phí yêu cầu cho việc duy trì và vận hành/quản lý những nguồn này. Cần kiểm tra cả chi phí ban đầu và chi phí hoạt động.

(6) Xem xét so sánh

Bằng cách so sánh "tình hình hiện tại", "CSIRT sẽ được thành lập" và "ứng cứu Sự cố lý tưởng", tổ chức có thể làm rõ việc thành lập CSIRT và có định hướng cho việc phát triển CSIRT sau khi hoạt động.

- **Xác định những vấn đề khi thành lập CSIRT bằng cách so sánh tình hình hiện tại với tình hình sau khi đã thành lập CSIRT**

  Bằng cách so sánh tình hình trước và sau khi đã thành lập CSIRT, ta có thể xác định những vấn đề chi tiết cần thực hiện trong quá trình thành lập CSIRT và tập trung thực hiện chúng.

  Việc mô phỏng ứng cứu Sự cố theo những kịch bản Sự cố lấy từ các Sự cố thực

---

các hoạt động để phát triển những chính sách và quy trình để đối phó với những Sự cố bằng cách thu thập và phân tích thông tin liên quan đến Sự cố, thông tin dễ bị tấn công và thông tin dự báo về những cuộc tấn công. (http://www.nca.gr.jp/)

tế đã xảy ra sẽ giúp xác định một cách hiệu quả những vấn đề thực hiện cụ thể trong và sau khi thành lập CSIRT. Ngoài ra, nếu một tình huống mô phỏng phát hiện ra bất kỳ khiếm khuyết nào trong kế hoạch của tổ chức, ta cũng có thể xem xét lại kế hoạch.

- **Xem xét những khác biệt giữa CSIRT lý tưởng và CSIRT sẽ được thành lập**

  Nếu CSIRT được thành lập không đáp ứng việc ứng cứu Sự cố do nguồn lực giới hạn hoặc do những hạn chế trong công ty, thì độ lệch so với CSIRT lý tưởng cần được xem. Vấn đề đó sẽ trở thành một điểm cần cải thiện sau khi CSIRT bắt đầu hoạt động, đem lại cho tổ chức những hướng dẫn hoạt động trung hạn và dài hạn để tiếp cận gần hơn với CSIRT lý tưởng.

(7) Kiểm tra tiến độ thành lập CSIRT

Chuẩn bị tài liệu giải thích về kế hoạch thành lập CSIRT để giúp nhận thức về sự cần thiết phải có một CSIRT trong công ty, bằng cách chọn ra những vấn đề đã được kiểm tra và cho thấy những lợi ích của các hoạt động CSIRT.

Chuẩn bị tài liệu cho từng nội dung sau:

- **Cấp quản lý / Cấp ra quyết định**
  - Tài liệu để phê duyệt việc thành lập CSIRT
- **Các bộ phận liên quan đến việc phản ứng Sự cố**
  - Tài liệu cho việc phối hợp nội bộ
- **Đối tượng phục vụ**
  - Tài liệu mô tả về CSIRT
- **Thành viên/Nhân viên của CSIRT**
  - Tài liệu để duy trì tổ chức CSIRT nội bộ

BƯỚC 3 Thành lập CSIRT

(1) Đảm bảo phê duyệt từ cấp quản lý / cấp ra quyết định và các nguồn lực
(2) Thực hiện phối hợp nội bộ
(3) Giải thích cho đối tượng phục vụ
(4) Thiết lập mô hình cho CSIRT
(5) Chuẩn bị những tài liệu cần thiết

Thành lập một CSIRT trong BƯỚC 3 dựa trên kế hoạch thành lập CSIRT đã chuẩn bị trong BƯỚC 2:

(1) Đảm bảo việc phê duyệt từ cấp quản lý / cấp ra quyết định và các nguồn lực

Có được phê duyệt từ cấp quản lý / cấp ra quyết định về kế hoạch thành lập CSIRT đã chuẩn bị trong BƯỚC 2, và đồng thời, đảm bảo có đầy đủ các nguồn lực để thành lập CSIRT.

(2) Thực hiện phối hợp nội bộ

Phối hợp với những bộ phận khác nhau liên quan đến việc phản ứng Sự cố, và thiết lập một mô hình hoạt động để CSIRT có thể thực hiện chức năng của mình.

(3) Giải thích cho đối tượng phục vụ

Giải thích cho đối tượng phục vụ về việc thành lập và hiểu về CSIRT, làm rõ những nhu cầu của đối tượng phục vụ, và xem xét yếu tố này có cần được phản ánh trong định hướng hoạt động của việc thành lập CSIRT hay không.

(4) Thiết lập mô hình hoạt động CSIRT

Thiết lập mô hình hoạt động cho CSIRT, chuẩn bị nguồn lực và đào tạo nhân viên.

(5) Chuẩn bị những tài liệu cần thiết

Chuẩn bị tài liệu cho các hoạt động của CSIRT với nội dung để giải thích về kế hoạch thành lập CSIRT và sử dụng như là tài liệu nội bộ. Chuẩn bị tài liệu phát thảo về CSIRT và cũng như tài liệu cần thiết cho việc vận hành CSIRT. Đối tới tài liệu phát thảo CSIRT, xem " Phụ lục (6) Các Tài liệu - Hướng dẫn Thành lập CSIRT".

Những tài liệu dùng cho việc vận hành CSIRT cần thiết thực, ví dụ như những tài liệu về mô hình hoạt động trong CSIRT, quy trình, nguyên tắc và hướng dẫn ứng cứu Sự cố cần được tuân thủ trong khi thực hiện nhiệm vụ, các đầu mối liên hệ, v.v...

Nếu khả năng phát sinh bất kỳ trở ngại nào trong việc thành lập CSIRT, xem xét lại kế hoạch thành lập CSIRT tối ưu cho tổ chức.

BƯỚC 4 Chuẩn bị trước khi vận hành CSIRT

✓ Thực hiện các mô phỏng

BƯỚC 4 là tạo ra các kịch bản Sự cố dựa trên những sự cố đã xảy ra thực tế và những sự cố dự kiến, thực hiện mô phỏng trên máy tính về các hoạt động của CSIRT. Những mô phỏng này giúp xác nhận sự hữu ích của CSIRT sẽ được thành lập và xác định các vấn đề có thể xảy ra trước khi bắt đầu hoạt động. Những vấn đề cần xác định gồm cơ chế phối hợp nội bộ, kênh thông tin liên lạc, và phân chia trách nhiệm. Đại diện tổ chức có liên quan tới ứng cứu Sự cố cần có mặt trong các hoạt động mô phỏng để đảm bảo việc thực hiện được hiệu quả.

Phải tiến hành hoạt động kiểm tra để xác định các điểm cần cải thiện sau khi thực hiện mô phỏng, và phản ánh kết quả trong tài liệu được chuẩn bị ở BƯỚC 3.

BƯỚC 5 Bắt đầu các hoạt động của CSIRT

(1) Phổ biến thông tin
(2) Cung cấp các dịch vụ CSIRT cho các bên nhận dịch vụ
(3) Thiết lập cơ chế phối hợp với bên ngoài

Trong BƯỚC 5, bắt đầu các hoạt động của CSIRT sau khi đã thực hiện theo BƯỚC 4 của quy trình thành lập.

(1) Phổ biến thông tin

Tổ chức phải thông báo cho các đối tượng phục vụ và đơn vị bên ngoài về sự tồn tại của CSIRT. Ngoài ra, cần cung cấp đầu mối liên hệ vận hành CSIRT. Sử dụng thông cáo báo chí là cách hiệu quả để các đơn vị bên ngoài biết được về CSIRT.

(2) Cung cấp các dịch vụ CSIRT cho các bên nhận dịch vụ

CSIRT thực sự hoạt động khi nó cung cấp dịch vụ cho đối tượng phục vụ, giảm thiểu những rủi ro kinh doanh thông qua việc ứng cứu Sự cố.

(3) Thiết lập cơ chế phối hợp với bên ngoài

Thiết lập cơ chế phối hợp với bên ngoài đã được kiểm tra ở BƯỚC 2 nhằm giảm thiểu những rủi ro kinh doanh.

Một khi các hoạt động CSIRT đã bắt đầu, Dự án Thành lập CSIRT xem như đã đạt được các mục tiêu. BƯỚC 6 tiếp theo sẽ mô tả những hoạt động thực tế của CSIRT.

BƯỚC 6 Soát xét

Trong BƯỚC 6, thực hiện soát xét các chức năng của CSIRT đã được hoạt động ở BƯỚC 5. Hoạt động soát xét cần được thực hiện định kỳ sau khi bắt đầu hoạt động để cải thiện chất lượng cũng như nâng cấp và tăng cường các chức năng của CSIRT. Tổ chức cần thực hiện việc soát xét dựa trên kết quả phân tích các hoạt động của chính CSIRT đó, hiểu những nhu cầu của đối tượng phục vụ, và những mô phỏng bạn đã thực hiện. Ngoài ra, cần nhớ rằng CSIRT phải luôn phát triển vì nó hoạt động trong môi trường bảo mật máy tính - môi trường liên tục phát triển. Ngoài ra, tổ chức phải tìm cách tạo ra một cơ chế hiệu quả trong việc phối hợp hoạt động liên tục với các đơn vị bên ngoài.

5 Lời kết

Đảm bảo an toàn cho máy tính không bao giờ là đủ. Việc thành lập CSIRT chỉ đơn thuần là một biện pháp giảm thiểu những rủi ro do Sự cố, biện pháp ứng phó hiệu quả cho các tổ chức để ngăn ngừa và phản ứng với các sự cố bảo mật. Nhiệm vụ của Hiệp hội CSIRT Nhật Bản là hỗ trợ các hoạt động thành lập CSIRT tại Nhật Bản. Các câu hỏi nếu có, vui lòng liên hệ với chúng tôi theo thông tin bên dưới.

< Thông tin liên hệ đến Hiệp hội CSIRT Nhật Bản >

Trung tâm Điều phối JPCERT
Tầng 11 toà nhà Hirose, 3-17 Kanda-Nishiki-cho, Chiyoda-ku,
Tokyo 101-0054
Email: nca-sec@nca.gr.jp
Điện thoại: +81-3-3518-4600
(Gặp Đại diện ban thư ký của Nippon CSIRT Association)

< Thông tin liên hệ đến VNCERT Vietnam >

Trung tâm Ứng cứu Khẩn cấp Máy tính ViệtNam
Toà nhà Cục Tần Số, 115 Trần Duy Hưng, Q, Cầu Giấy, Hà Nội,
Việt Nam
Email: ir@vncert.vn
Điện thoại +84-4-3640-4421

Danh sách các Tác giả và Cộng tác viên

Hajime Ishizuka	NTT Communications
Kunihiko Sakuma	JSOL Corporation
Kaori Sagawa	KLIRRT
Motoki Sone	Sharp Corporation
Masahito Yamaga	Thành viên của NCA Expert Committee
Tomotaka Shoji	TOPPAN-CERT
Yoshinari Fukumoto	Rakuten-CERT
Yusuke Gunji	Rakuten-CERT
Yoshitane Tachibana	OKI-CSIRT
Akiko Numata	HIRT
Masato Terada	HIRT
Yuki Shigeiwa	Phòng Cơ sở hạ tầng IT, Bộ phận Quản lý Hệ thống, DeNA Co., Ltd.
Yoshiki Sugiura	NTT-CERT
Ikuya Hayashi	NTT-CERT
Takahiko Yoshida	NTT-CERT

Translated into English by

NTT EAST Corporation
VNCERT

Translated into Vietenamiese by

NTT EAST Corporation
VNCERT

Dịch và hoàn thiện bản tiếng Việt

Trần Tuấn Anh	VNCERT
Đăng Huy Hoàng	VNCERT
Nguyễn Thị Thu Huyến	VNCERT
Nguyễn Trung Kiên	VNCERT
Nguyễn Hữu Nguyên	VNCERT

Phụ lục cho Hướng dẫn Thành lập CSIRT

(1) Chi tiết về thông tin cần thu thập, tình hình hiện tại, và các vấn đề cần được xác định

Đề mục chính	Đề mục phụ	Dự kiến sử dụng thông tin
Hiểu những mục tiêu cần bảo vệ và những mối đe dọa	Mạng & hệ thống nội bộ - Quản trị viên phụ trách vận hành - Những hệ thống quan trọng - Tài sản thông tin	Những tài liệu để ra quyết định về những Sự cốcần xử lý bởi CSIRT
	Thông tin về những Sự cố trong quá khứ - Sự cố nghiêm trọng đã xảy ra - Những Sự cố có khuynh hướng tái diễn	
	Kết quả phân tích về những rủi ro đang tồn tại	
Cơ chế phản ứng Sự cố hiện tại	Hoạt động ngăn ngừa các Sự cố hiện tại - Tổ chức chịu trách nhiệm vận hành / cơ chế phối hợp giữa các bộ phận / các quy trình	Xác định những vấn đề và những điểm cần cải thiện trong chức năng và mô hình phản ứng Sự cố hiện tại
	Hoạt động xử lý các Sự cố hiện tại - Tổ chức chịu trách nhiệm vận hành / cơ chế phối hợp giữa các bộ phận / các quy trình	
	Những nỗ lực để tăng cường bảo mật hiện tại - Tổ chức chịu trách nhiệm vận hành / cơ chế phối hợp giữa các bộ phận / các quy trình	
	Những tổ chức bên ngoài tham gia vào phản ứng Sự cố hiện tại	Thiết lập cơ chế phối hợp hiệu quả với bên ngoài trong việc phản ứng Sự cố
	Thiết lập cơ chế phối hợp hiệu quả với bên ngoài về phản ứng Sự cố	
Chính sách bảo mật và các tài liệu liên quan đến bảo mật hiện tại	Chính sách bảo mật	Hiểu những hạn chế trong việc phản ứng Sự cố
	Kế hoạch khôi phục thảm hoạ / Kế hoạch duy trì kinh doanh	
	Những hạn chế và quy định liên quan đến bảo mật	
	Những hạn chế liên quan đến bảo mật vật lý	
Thông tin tham khảo	Thông tin về những CSIRT khác[7]	Thông tin tham khảo cho việc thành lập CSIRT

Bảng 2: Thông tin được thu thập ở BƯỚC 1

[7] Thông tin về những CSIRT hàng đầu trên thế giới: FIRST (http://www.first.org/), APCERT (http://www.apcert.org/) được cung cấp bởi Nippon CSIRT Association .(http://www.nca.gr.jp/).

(2) Phân loại sự cố

Dò, quét, hay bất kỳ truy cập khả nghi khác	• Tìm kiếm những điểm yếu (ví dụ như kiểm tra phiên bản của những phần mềm trên máy chủ) • Các nỗ lực xâm nhập (không thành công) • Các nỗ lực lây nhiễm worm (không thành công)
Chuyển tiếp trái phép các phần mềm máy chủ	• Sử dụng máy chủ mail hay proxy của các bên thứ ba mà không có sự đồng ý của quản trị viên
Truy cập khả nghi	• Mạo danh người gửi
Xâm nhập vào hệ thống	• Xâm nhập vào các hệ thống, giả mạo (bao gồm sử dụng phần mềm kiểm soát máy tính (rootkit) hay bất kỳ công cụ chuyên dụng nào khác) • Thiết lập chương trình cho các cuộc tấn công DDoS (chuyển hướng bên thứ ba)
Tấn dẫn từ chối dịch vụ (DoS)	• Làm nghẽn mạng • Dừng các chương trình trên máy chủ • Treo hay khởi động lại hệ điều hành máy chủ
Nhiễm worm / virus máy tính	
Các sự cố khác	• Nhận thư quảng cáo không mong muốn (UCE – unsolicited Commercial E-mail), gọi là thư rác

Bảng 3: Phân loại những Sự cố điển hình chính

(3) Dịch vụ

Các dịch vụ của CSIRT có thể được chia thành ba loại chính:

1) Dịch vụ khắc phục Sự cố

Xử lý Sự cố nhằm mục đích giới hạn thiệt hại do các Sự cố gây ra.

2) Dịch vụ ngăn ngừa Sự cố

Những dịch vụ phát hiện, giảm thiểu khả năng xảy ra Sự cố và sự kiện Bảo mật[8] nhằm mục đích ngăn các Sự cố xảy ra.

3) Dịch vụ tăng cường chất lượng bảo mật

Những dịch vụ nhằm tăng cường chất lượng bảo mật nội bộ. Chúng cung cấp hiểu biết về quan điểm và chuyên môn của CSIRT nhằm để các hoạt động có thể được thực hiện qua sự phối hợp với các tổ chức nội bộ. Các dịch vụ này cũng có thể gián tiếp ngăn ngừa xảy ra Sự cố.

Bảng 4 thể hiện danh sách những dịch vụ CSIRT điển hình, CSIRT không nhất thiết phải có tất cả các dịch vụ này và trong một số trường hợp có thể đưa thêm những dịch vụ khác.

Dịch vụ khắc phục sự cố	Dịch vụ ngăn ngừa sự cố	Dịch vụ tăng cường chất lượng bảo mật
• Xử lý Sự cố • Điều phối • Ứng cứu Sự cố tại chỗ • Hỗ trợ ứng cứu sự cố • Điều tra số máy tính • Xử lý nhân công	• Cung cấp thông tin liên quan đến bảo mật • Xử lý thông tin lỗ hổng • Phát hiện Sự cố / Tình huống Bảo mật • Khảo sát xu hướng kỹ thuật • Đánh giá / kiểm tra bảo mật • Phát triển công cụ bảo mật	• Phân tích / đánh giá rủi ro • Chuẩn bị và sửa đổi những kế hoạch duy trì kinh doanh, khôi phục thảm hoạ • Tư vấn bảo mật • Các hoạt động giáo dục / đào tạo / hướng dẫn về bảo mật • Đánh giá / Chứng nhận sản phẩm

Bảng 4: Phác thảo về các Dịch vụ CSIRT

Chi tiết về các dịch vụ như sau:

1) CÁC DỊCH VỤ KHẮC PHỤC SỰ CỐ

- Xử lý Sự cố

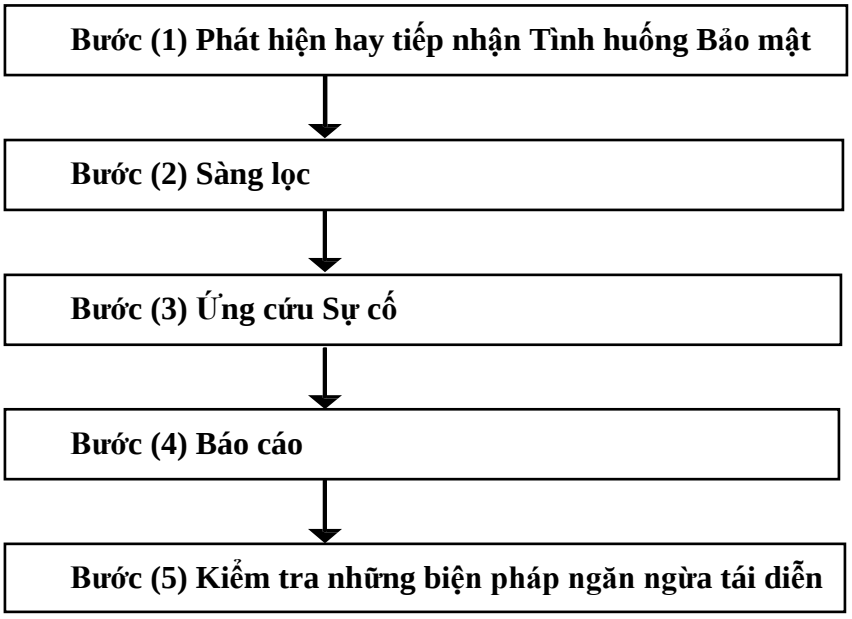
  Xử lý Sự cố là chức năng cơ bản của CSIRT và cần được thực hiện mà không được sai sót. Nó là hoạt động ứng cứu cho các Sự cố thực tế nhằm mục đích hạn chế thiệt hại và khôi phục.

  Xử lý Sự cố cần được thiết lập thành quy trình cho CSIRT.

  Hình dưới đây thể hiện trình tự điển hình các bước xử lý Sự cố, là cơ sở cho

[8] Với mục đích của tài liệu này, "Sự kiện Bảo mật" được định nghĩa là một sự kiện có khả năng, nhưng chưa được xác nhận là một Sự cố.

việc chuẩn bị xây dựng các quy trình.



Hình 4: Trình tự cơ bản của các bước Xử lý Sự cố

Phần sau đây mô tả chi tiết trình tự.

(1) Phát hiện hay tiếp nhận những sự kiện Bảo mật[9]

Bước này liên quan đến việc nhận và quản lý các báo cáo về sự kiện Bảo mật.

(2) Sàng lọc[10]

Sàng lọc là quyết định một sự kiện Bảo mật có là một Sự cố hay không và đặt mức độ ưu tiên cho Sự cố.

Trong bước này, cần xác định đúng các tiêu chí để sàng lọc. Tuy nhiên, các tiêu chí cần được xem xét theo định kỳ vì những yếu tố hình thành nên các tiêu chí liên tục thay đổi theo việc môi trường bảo mật máy tính – môi trường đang phát triển rất nhanh chóng.

Xem xét những điểm sau đây và thực hiện sàng lọc trên cơ sở những tiêu chí đã xác định:

- Xác thực sự thật của tình huống.
- Đánh giá mức độ ảnh hưởng.

Nên gán định danh cho mỗi Sự cố được sàng lọc để dễ dàng tham khảo về sau.

[9] Vì mục đích của tài liệu này, "Tình huống Bảo mật" được định nghĩa là một sự kiện có khả năng, nhưng chưa được xác định chính xác là một Sự cố.

[10] Sàng lọc là một thuật ngữ được sử dụng trong y học. Thuật ngữ này được sử dụng khi đề cập đến việc ưu tiên chữa trị cho bệnh nhân dựa trên tính khẩn cấp phải điều trị để cứu được nhiều mạng sống nhất khi các nguồn lực bị hạn chế.

(3) Ứng cứu Sự cố

Ứng sự cố là một hoạt động điều tra để xác định nguyên nhân của Sự cố và thực hiện các nỗ lực khôi phục. Vì vậy, phải phân tích Sự cố đã được sàng lọc và xác định bản chất của Sự cố.

Các yếu tố đặc trưng cho Sự cố:

- Kẻ tấn công
- Mục tiêu tấn công
- Ngày xảy ra Sự cố
- Phương pháp tấn công
- Mức độ tác động
- Nguyên nhân chính của thiệt hại
- Những biện pháp có thể được thực hiện
- Khả năng lan rộng thiệt hại

Dựa trên các yêu tố đã liệt kê ở trên, xác định và thực hiện các biện pháp ứng cứu phù hợp.

Những chức năng điển hình của CSIRT trong ứng cứu Sự cố như sau:

- **Điều phối**

  Đôi khi, việc xử lý Sự cố yêu cầu phải có sự phối hợp của nhiều tổ chức nội bộ và bên ngoài theo trách nhiệm. CSIRT được mong đợi sẽ đóng vai trò là người điều phối do hiểu được bức tranh tổng thể về Sự cố, đảm bảo việc xử lý Sự cố thống nhất và hiệu quả. Ứng cứu Sự cố kịp thời yêu cầu phải có điều phối ngay lập tức.

- **Ứng cứu Sự cố tại chỗ**

  CSIRT sẽ trực tiếp thực hiện việc khôi phục cho hệ thống hoặc mạng ở tại nơi xảy ra Sự cố. Cần thiết lập việc phân chia trách nhiệm giữa CSIRT và người phụ trách vận hành hệ thống.

- **Hỗ trợ ứng cứu Sự cố**

  CSIRT sẽ hỗ trợ ứng cứu sự cố qua e-mail và/hoặc điện thoại, cung cấp tài liệu và những phương thức khác.

- **Điều tra số máy tính**

  Tiến hành xử lý Sự cố bằng cách sao lưu và bảo toàn dữ liệu khỏi máy tính bị Sự cố, giúp cung cấp bằng chứng và phân tích, ví dụ: (1) loại thiệt hại nào đã xảy ra; (2) kẻ xâm nhập vào ở vị trí nào; và (3) kẻ xâm nhập là ai. CSIRT cần có thành viên là những người có kỹ năng chuyên môn, và được trang bị các công cụ chuyên dụng về điều tra số máy tính. Ngoài ra, lưu ý phải kiểm soát chặt chẽ thông tin phục vụ điều tra bên trong CSIRT.

- **Xử lý nhân công**

  Bước này bao gồm các dịch vụ để phân tích các chương trình khả nghi được phát hiện qua việc xử lý Sự cố. Tiến hành điều tra để xác định liệu chương trình khả nghi có gây ra Sự cố hay qua thông qua một phân tích về mã nguồn, phân tích hành vi trong môi trường cách ly. CSIRT cần có các thành viên có kỹ năng chuyên môn, và được trang bị những trang thiết bị

chuyên dụng tách biệt với các mạng khác.

(4) Báo cáo

Báo cáo là kết quả của việc xử lý Sự cố sau khi đã điều tra những nguyên nhân của Sự cố và thực hiện nỗ lực khôi phục. Ví dụ báo cáo có thể được sử dụng để tích lũy phương pháp xử lý Sự cố trong CSIRT và đưa ra các báo cáo cho người bị Sự cố[11] và các cá nhân / bộ phận nhận khác trong nội bộ.

(5) Kiểm tra những biện pháp ngăn ngừa sự lặp lại

Cần phải phân tích nguyên nhân các Sự cố đã được giải quyết và thực hiện các biện pháp ngăn ngừa sự lặp lại. Trong quá trình phân tích Sự cố, bạn cần chọn ra các nội dung sau đây một lần nữa:

- Chi tiết về Sự cố:
  - Nguyên nhân
  - Tình hình thiệt hại
  - Thời điểm phát hiện Sự cố
  - Các biện pháp ban đầu / tạm thời
  - Các biện pháp lâu dài
- Những tổ chức liên quan đến xử lý Sự cố
- Những điểm được và/hoặc chưa được về xử lý Sự cố

Bạn cần thực hiện các biện pháp ngăn ngừa sự lặp lại, dựa trên kết quả phân tích.

2) CÁC DỊCH VỤ PHẢN ỨNG NGĂN NGỪA SỰ CỐ

- **Cung cấp / thông báo thông tin liên quan đến bảo mật**

  Dịch vụ này cung cấp thông tin bảo mật cho đối tượng phục vụ. Ví dụ sau đây là những thông tin được cung cấp:
  - Thông tin được phổ biến về những hoạt động của CSIRT / thông tin liên hệ.
  - Chính sách / quy trình/ danh sách kiểm tra liên quan đến bảo mật
  - Thông tin về virus / worm và các phương pháp tấn công phổ biến
  - Những phương pháp điển hình về phản ứng Sự cố
  - Thống kê Sự cố
- **Xử lý thông tin lỗ hổng[12]**

  Dịch vụ này dùng để phân tích thông tin về những lỗ hổng phần mềm và phần cứng, và truyền đạt lại cho đối tượng phục vụ. Đối tượng phục vụ phải quản lý việc ứng dụng các bản vá lỗi để sửa chữa các lỗ hổng và việc thực hiện các giải pháp thay thế. Trong quá trình xử lý thông tin lỗ hổng, bạn phải hiểu loại phần

[11] Tổ chức hay cá nhân gặp Sự cố.

[12] Sau đây là một số ví dụ về những URL sẽ được dùng làm những tham khảo hữu ích cho việc thu thập thông tin lỗ hổng.
- Security Focus (http://securityfocus.com/)
- Secunia (http://secunia.com/)
- SANS Handler's Diary (http://isc.sans.org/diary.php)
- FrSIRT (http://www.frsirt.com/english/)
- JVN (http://jvn.jp/index.html)

mềm và phần cứng được đối tượng phục vụ sử dụng.

Trong trường hợp phát hiện thấy những lỗ hổng trong sản phẩm tự phát triển, dịch vụ này phải xử lý các lỗ hổng đó.

- **Phát hiện Sự cố / Sự kiện Bảo mật**

  Dịch vụ này dùng để phát hiện những Sự cố / Sự kiện Bảo mật, v.v… Phương pháp phát hiện gồm việc cài đặt các hệ thống phát hiện xâm nhập (IDS), hoặc honeypot, phân tích nhật ký của các máy chủ khác nhau, và môi trường chuyên dụng để phát hiện rò rỉ thông tin thông qua các ứng dụng chia sẻ tập tin ngang hàng (P2P - peer-to-peer).

- **Khảo sát xu hướng kỹ thuật**

  Dịch vụ này để khảo sát các xu hướng, và đưa ra những ý kiến chuyên môn về những công nghệ bảo mật mới nhất, như các công nghệ tăng cường bảo mật, công nghệ phát hiện Sự cố, hoặc kỹ thuật xâm nhập và xác minh tính hữu ích cho đối tượng phục vụ. Thực hiện những công nghệ hữu ích trong CSIRT và sử dụng chúng để cung cấp thông tin cho đối tượng phục vụ.

  - Đánh giá / kiểm tra bảo mật

    Các dịch vụ đánh giá / kiểm tra thông qua kiểm tra tài liệu hay kiểm thử xâm nhập (penetration testing).

  - Phát triển công cụ bảo mật

    Dịch vụ phát triển các công cụ sẽ được CSIRT hay đối tượng phục vụ sử dụng. Ví dụ, dịch vụ này phát triển những công cụ phát hiện Sự cố mới hay những script để làm cho các công nghệ mã hóa dễ sử dụng hơn, hoặc tự động hóa việc phân phối bản vá.

3) CÁC DỊCH VỤ TĂNG CƯỜNG CHẤT LƯỢNG BẢO MẬT

- **Phân tích / đánh giá rủi ro**

  Dịch vụ này nhằm xác định những rủi ro khác nhau có thể gây trở ngại đến tính bảo mật, tính toàn vẹn và tính sẵn sàng của một doanh nghiệp hay hệ thống thông tin, và phân tích các tác động của nó. Dịch vụ này được dùng để phát hiện và giảm thiểu những rủi ro hiện tại.

  Nhìn chung, dịch vụ này bao gồm:

  - Xác định những tài sản thông tin (sắp xếp ưu tiên)
  - Phân tích rủi ro đối với những tài sản đã xác định

  Có thể giảm hiểu rủi ro bằng cách thể hiện trong các chính sách bảo mật, dịch vụ CSIRT, quy trình xử lý Sự cố, v.v… trên cơ sở phân tích rủi ro.

- **Chuẩn bị và sửa đổi các kế hoạch duy trì kinh doanh, khôi phục thảm hoạ**

  Dịch vụ này phản ánh những chức năng ứng cứu Sự cố của CSIRT trong các chiến lược quản lý về các kế hoạch duy trì kinh doanh liên tục và khôi phục thảm hoạ, bảo vệ công ty không đánh mất các giao dịch khách hàng vào tay đối thủ cạnh tranh, giảm thị phần, hay giảm giá trị doanh nghiệp bằng cách không

để bất kỳ Sự cố nào làm gián đoạn các kinh doanh quan trọng, hay bằng cách khôi phục kinh doanh sớm nhất có thể, thậm chí trong trường hợp việc kinh doanh đã bị gián đoạn.

- **Tư vấn bảo mật**

  Dịch vụ tư vấn này phản ánh bí quyết của CSIRT trong các mảng kinh doanh của đối tượng phục vụ. Các bí quyết có thể được sử dụng để đáp ứng các yêu cầu bảo mật trong kinh doanh, hoặc bản thân các bí quyết cũng có thể là một hoạt động kinh doanh. Các bí quyết được sử dụng như thế nào sẽ tùy vào các lĩnh vực kinh doanh khác nhau của công ty.

- **Các hoạt động giáo dục / đào tạo / hướng dẫn về bảo mật**

  Dịch vụ này nhằm mục đích giáo dục, đào tạo và hướng dẫn đối tượng phục vụ thông qua các hội nghị chuyên đề, hội thảo, khóa học, tài liệu hướng dẫn, hoặc bằng phương pháp riêng của CSIRT, cũng như các chính sách / quy trình và các nội dung khác phản ánh các bí quyết . Dịch vụ này thường được phối hợp với phòng phát triển nhân lực hoặc bộ phận tương đương để cung cấp.

- **Đánh giá / chứng nhận sản phẩm**

  Với dịch vụ này, CSIRT đánh giá và chứng nhận các sản phẩm, công cụ, dịch vụ, … bằng cách xác định liệu đối tượng phục vụ có thể sử dụng các hạng mục này an toàn hay không. CSIRT cần thiết lập các tiêu chí đánh giá và chứng nhận phù hợp với tổ chức.

(4) Các bộ phận tham gia vào các hoạt động CSIRT

Cấp quản lý / Cấp ra quyết định	Đảm bảo kinh phí và các nguồn lực, phản ánh nhiệm vụ và thẩm quyền được CSIRT vào các hệ thống nội bộ qua việc phê duyệt thành lập CSIRT. Cấp này là đối tượng nhận báo cáo Sự cố sau cùng.
Phòng/Bộ phận phụ trách quản lý / vận hành các hệ thống thông tin	Bộ phận này tham gia sâu vào các hoạt động CSIRT, trong một số trường hợp bộ phận này sẽ đóng vai trò là đối tượng nhận dịch vụ và có thể có chức năng xử lý Sự cố.
Phòng/Bộ phận kiểm soát nội bộ	Phối hợp ứng cứu Sự cố với các hoạt động kiểm soát nội bộ (lưu ý rằng các hoạt dộng của CSIRT chỉ nhằm phản ứng với Sự cố, không thực hiện các hoạt động kiểm soát nội bộ khác).
Phòng/Bộ phận pháp lý	Giải quyết những vấn đề pháp lý về phản ứng Sự cố.
Phòng/Bộ phận truyền thông	Giải quyết với báo chí về mặt phản ứng Sự cố.
Phòng/Bộ phận nhân sự	Chỉ định / tuyển dụng nhân viên CSIRT. Thực hiện các biện nhân sự tại nơi xảy ra Sự cố (lưu ý rằng các hoạt động của CSIRT chỉ nhằm phản ứng với Sự cố, không thực hiện các biện pháp về nhân sự khác).
Phòng/Bộ phận phát triển nhân sự	Giáo dục, đào tạo và hướng dẫn đối tượng phục vụ thông qua các hội nghị chuyên đề, hội thảo, khóa học, tài liệu hướng dẫn, hoặc bằng phương pháp riêng và chính sách bảo mật.
Phòng/Bộ phận kế hoạch	Thể hiện các kế hoạch duy trì kinh doanh / kế hoạch khôi phục thảm hoạ và phản ứng Sự cố.
Tổng đài hỗ trợ (help-desk)	Điểm liên hệ đầu tiên cho việc xử lý Sự cố.
Phòng/Bộ phận bảo vệ	Giải quyết việc trộm tài sản (đặc biệt là các máy tính). Quản lý và thực hiện kiểm soát truy cập.

Bảng 5: Ví dụ về các Bộ phận tham gia vào các hoạt động CSIRT

(5) Các nguồn lực

Phần sau đây phác thảo về những nguồn lực cần thiết.

● **Nhân lực**

CSIRT yêu cầu các nguồn nhân lực đóng những vai trò sau:

- Quản lý / Trưởng nhóm / Trưởng đội

  Những người chịu trách nhiệm giám sát hoạt động và ra quyết định cho đội hoặc nhóm.

- Nhân viên sàng lọc

  Những người thực hiện sàng lọc theo những tiêu chí đã được thiết lập và ưu tiên chỉ định những người xử lý cho Sự cố.

- Người xử lý Sự cố

  Nhân viên thực hiện xử lý sự cố cho các Sự cố đã được sàng lọc và hỗ trợ chủ chốt cho các thành viên CSIRT.

- Nhân viên khác cho dịch vụ cung cấp

  Nhân viên hỗ trợ thực hiện các hoạt động cung cấp dịch vụ.

Ví dụ về những kỹ năng được yêu cầu cho nhân viên như sau:

- Kỹ năng kỹ thuật cơ bản:
  - Các kỹ năng về Hệ điều hành (ví dụ như Windows, UNIX)
  - Kỹ năng mạng
  - Kỹ năng lập trình
  - Kỹ năng trong việc sử dụng mã hóa PGP (Pretty Good Privacy)
- Kỹ năng bảo mật:
  - Kỹ năng liên quan đến tấn công máy tính / các lỗ hổng
  - Kinh nghiệm và kỹ năng xử lý Sự cố
- Kỹ năng cá nhân:
  - Kỹ năng phối hợp
  - Kỹ năng giao tiếp
  - Khả năng xử lý sự cố

Những kỹ năng này thôi vẫn chưa đủ vì chúng chỉ là những kỹ năng cơ bản. CSIRT đặc biệt cần các nhân viên có các kỹ năng chuyên sâu cho từng dịch vụ được CSIRT cung cấp.

● **Nguồn lực trang thiết bị**

Ví dụ về các nguồn lực trang thiết bị được thể hiện dưới đây:

- Các thiết bị văn phòng cơ bản:
  - Điện thoại dùng riêng cho CSIRT

- Máy tính cho nhân viên (với môi trường làm việc an toàn như mã hóa PGP)
- Điện thoại di động cho nhân viên
- Máy in chuyên dụng
- Máy hủy giấy chuyên dụng, v.v…

- Cơ sở hạ tầng cho CSIRT:
  - Văn phòng cho CSIRT có kiểm soát ra vào
  - Môi trường mạng cho CSIRT
  - Két sắt
  - Hệ thống xử lý Sự cố[13]
  - Máy tính cá nhân có thể được mang đi xử lý Sự cố
  - Cơ sở hạ tầng yêu cầu cho việc cung cấp dịch vụ, v.v…

[13] Hệ thống xử lý Sự cố dùng thay cho bộ dụng cụ để thu thập, phân tích, và chia sẻ thông tin Sự cố.

(6) Tài liệu

Các mẫu tài liệu phác thảo cho CSIRT được quy định trong RFC2350[14]. Chúng tôi khuyến nghị bạn nên chuẩn bị tài liệu theo các mẫu này.

---

1 Thông tin tài liệu
- 1.1 Ngày cập nhật gần nhất
- 1.2 Danh sách phân phối
- 1.3 Những nơi mà tài tiệu có thể tìm thấy (nơi lưu trữ / sử dụng / tra cứu)

2 Thông tin liên hệ
- 2.1 Tên nhóm
- 2.2 Địa chỉ
- 2.3 Múi giờ
- 2.4 Số điện thoại
- 2.5 Số fax
- 2.6 Thông tin liên lạc khác
- 2.7 Địa chỉ thư điện tử
- 2.8 Mã hóa và khóa công cộng
- 2.9 Thành viên trong nhóm
- 2.10 Thông tin khác
- 2.11 Thông tin liên hệ khách hàng

3 Điều lệ
- 3.1 Tuyên bố nhiệm vụ
- 3.2 Đối tượng phục vụ
- 3.3 Tài trợ và/hoặc sát nhập
- 3.4 Thẩm quyền

4 Chính sách
- 4.1 Loại Sự cố và mức độ hỗ trợ
- 4.2 Phối hợp, tương tác và chia sẻ thông tin
- 4.3 Thông tin liên lạc và xác thực

5 Dịch vụ
- 5.1 Phản ứng Sự cố
  - 5.1.1 Sàng lọc Sự cố
  - 5.1.2 Phối hợp về Sự cố
  - 5.1.3 Giải pháp cho Sự cố
- 5.2 Hoạt động chủ động trước sự cố

6 Các mẫu báo cáo Sự cố

7 Sự từ chối

---

[14] http://www.ietf.org/rfc/rfc2350.txt (Tiếng Anh)

http://www.ipa.go.jp/security/rfc/RFC2350JA.html (Tiếng Nhật)